DISEÑO RED INALÁMBRICA PAUs TRANSMILENIO S.A.

LADYS GISSELA OSPINO OROZCO

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO- MECÁNICAS
ESCUELA DE INGENIERÍAS ELÉCTRICA ELECTRÓNICA Y TELECOMUNICACIONES.
BUCARAMANGA
2006

DISEÑO RED INALÁMBRICA PAUs TRANSMILENIO S.A.

LADYS GISSELA OSPINO OROZCO

Informe de Práctica Empresarial para optar al título de Ingeniera Electrónica

Director
Magíster JORGE HERNANDO RAMÓN SUÁREZ
UIS

Tutor
Ing. WILMER GALINDO ARIAS
TechLAN Solutions Ltda.

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO- MECÁNICAS
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
BUCARAMANGA
2006

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

GLOSARIO

802.11: 802.11, o IEEE 802.11, es un grupo de trabajo del IEEE que desarrolla distintos estándares para el uso de la tecnología de radiofrecuencia en las redes de área local (LAN).
802.11 se compone de distintas normas que operan a diferentes frecuencias, con distintas velocidades y capacidades.

802.1X: la IEEE 802.1X es una norma de la IEEE para Control de Admisión de Red basada en puertos. Es parte del grupo de protocolos IEEE 802 (IEEE 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla. Es utilizado en algunos puntos de acceso inalámbricos cerrados y se basa en protocolo de autenticación extensible (EAP– RFC 2284).
Algunos proveedores están implementando 802.1X en puntos de acceso inalámbricos que pueden utilizarse en ciertas situaciones en las cuales el punto de acceso necesita operarse como un punto de acceso cerrado, corrigiendo fallas de seguridad de WEP. Esta autenticación es realizada normalmente por un tercero, tal como un servidor de RADIUS. Esto permite la autenticación del solo cliente o, más apropiadamente, una autenticación mutua fuerte utilizando protocolos como EAP-TLS.

AES (Advanced Encryption Standard): algoritmo de encriptación del gobierno de EE.UU, basado en el algoritmo Rijndael, método de encriptación simétrica con clave de 128 bits desarrollada por los belgas Joan Daemen y Vincent Rijmen.

Access Point (AP, Punto de Acceso): estación base o "base station" que conecta una red cableada con uno o más dispositivos wireless.

Existen muchos tipos de Access Point en el mercado, con diferentes capacidades: bridge, hubs, gateway, router, y las diferencias entre ellos muchas veces no están claras, porque las características de uno se pueden incluir en otro. Por ejemplo, un router puede hacer bridge, y un hub puede hacer switch.

Además, los Access Points pueden mejorar las características de la WLAN, permitiendo a un cliente realizar roaming entre distintos AP de la misma red, o compartiendo una conexión a Internet entre los clientes wireless.

Autentificación: proceso de identificación de un equipo o usuario. El estándar 802.11 define dos métodos de autentificación: open system y shared key.

Bridge: dispositivo que conecta dos segmentos de red que emplean el mismo protocolo de red (por ejemplo, IP) pero con distintos medios físicos (por ejemplo, 802.11 y 10baseT).

CIFRADO: proceso mediante el cual los datos se codifican de tal manera que no pueden ser interpretados fácilmente. Es una medida de seguridad utilizada para que al momento de transmitir los datos éstos no puedan ser interceptados por intrusos.

DHCP, Dynamic Host Configuration Protocol: protocolo para la configuración automática de los parámetros de red de los equipos. La información se almacena en un servidor DHCP al que los equipos, al encenderse, solicitan los parámetros de configuración.

DSSS (Direct Sequence Spread Spectrum): el espectro ensanchado por secuencia directa también conocido en comunicaciones móviles como DS-CDMA (acceso múltiple por división de código en secuencia directa), es uno de los métodos de modulación en espectro ensanchado para transmisión de señales digitales sobre ondas radiofónicas que más se utilizan.

El espectro ensanchado por secuencia directa es una técnica de modulación que utiliza un código de pseudoruido para modular directamente una portadora, de tal forma que aumente el ancho de banda de la transmisión y reduzca la densidad de potencia espectral (es decir, el nivel de potencia en cualquier frecuencia dada). La señal resultante tiene un espectro muy parecido al del ruido, de tal forma que a todos los radiorreceptores les parecerá ruido menos al que va dirigida la señal.

FHSS (Frequency Hopping Spread Spectrum): es una técnica de modulación en espectro ensanchado en el que la señal se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia síncronamente con el transmisor.

IP, dirección: un número de 32 bits que identifica a un equipo a nivel de protocolo de red en el modelo ISO. Se compone de dos partes: la dirección de red, común a todos los equipos de la red, y la dirección del equipo, única en dicha red.

ISM, Industrial, Scientific and Medical band: bandas de frecuencias reservadas originalmente para uso no comercial con fines industriales, científicos y médicos. Posteriormente, se empezaron a usar para sistemas de comunicación tolerantes a fallos que no necesitaran licencias para la emisión de ondas.

802.11b y 802.11g operan en la ISM de los 2.4 GHz, así como otros dispositivos como teléfonos inalámbricos y hornos microondas, por ejemplo.

MAC (Media Access Control), dirección: en las redes wireless, el MAC es un protocolo de radiofrecuencia, corresponde al nivel de enlace (nivel 2) en el modelo ISO. Cada dispositivo wireless posee una dirección para este protocolo, denominada dirección MAC, que consiste en un número de 48 bits: los primeros 24 bits identifican al fabricante de la tarjeta, mientras que los restantes 24, a la tarjeta en sí. Este modelo de direccionamiento es común con las redes Ethernet (802.3).

Omnidireccional, antena: antena que proporciona una cobertura total en un plano (360 grados) determinado.

OFDM (Ortogonal Frequency Division Multiplexing): división de frecuencia por multiplexación ortogonal, Es una técnica de modulación FDM que permite transmitir grandes cantidades de datos digitales sobre una onda de radio. OFDM divide la señal de radio en muchas sub-señales que son transmitidas simultáneamente hacia el receptor en diferentes frecuencias. OFDM reduce la diafonía (efecto de cruce de líneas) durante la transmisión de la señal, OFDM se utiliza en 802.11a WLAN, 802.16, WiMAX y, en Europa, en PLC.

PoE (Power over Ethernet): es una tecnología que permite la alimentación eléctrica de dispositivos de red a través de un cable UTP / STP en una red ethernet. PoE se rige según el estándar IEEE 802.3af y abre grandes posibilidades cuando se requiere dar alimentación a dispositivos tales como cámaras de seguridad o puntos de acceso inalámbricos.
Actualmente existen en el mercado varios dispositivos de red como switches o hubs que soportan esta tecnología. Para implementar PoE en una red que no se dispone de dispositivos que la soporten directamente se usa una unidad base (con conectores RJ45 de entrada y de salida) con un adaptador de alimentación para recoger la electricidad y una unidad terminal (también con conectores RJ45) con

un cable de alimentación para que el dispositivo final obtenga la energía necesaria para su funcionamiento.

PSK (Phase Shift Keying): la modulación por desplazamiento de fase o PSK (Phase Shift Keying) es una forma de modulación angular consistente en hacer variar la fase de la portadora entre un número de valores discretos. La diferencia con la modulación de fase convencional (PM) es que mientras en ésta la variación de fase es continua, en función de la señal moduladora, en la PSK la señal moduladora es una señal digital y, por tanto, con un número de estados limitado.

QoS (Quality of Service): en Internet y otras redes, designa la posibilidad de medir, mejorar y, en alguna medida, garantizar por adelantado los índices de transmisión y error.

RADIUS: esquema de seguridad adicional de las redes WLAN que hace uso de un servidor equipado con una base de datos para autenticación de los usuarios móviles.

RC4: es el sistema de cifrado de flujo *Stream Cipher* más utilizado y se usa en algunos de los protocolos más populares como Transport Layer Security (TLS/SSL) (para proteger el tráfico de Internet) y Wired Equivalent Privacy (WEP) (para añadir seguridad en las redes inalámbricas). RC4 fue excluido en seguida de los estándares de alta seguridad por los criptógrafos y algunos modos de usar el algoritmo de criptografía RC4 lo han llevado a ser un sistema de criptografía muy inseguro, incluyendo su uso WEP. No está recomendado su uso en los nuevos sistemas, sin embargo, algunos sistemas basados en RC4 son lo suficientemente seguros para un uso común.

RIP (Routing Information Protocol): protocolo de información de encaminamiento. Es un protocolo utilizado por los routers para intercambiar información acerca de la red.

Roaming: nombre dado a la acción de moverse del área de cobertura de un Punto de Acceso a otro sin pérdida de conectividad, de forma que el usuario no lo percibe.

SSID, Service Set Identification: conjunto alfanumérico de hasta 32 caracteres que identifica a una red inalámbrica. Para que dos dispositivos wireless se puedan comunicar, deber tener configurado el mismo SSID, pero dado que se puede obtener de los paquetes de la red wireless en los que viaja en texto claro, no puede ser tomado como una medida de seguridad.
Dependiendo de si la red wireless funciona en modo Ad-Hoc o en modo Infraestructura, el SSID se denomina ESSID o BSSID.

TKIP, Temporal Key Integrity Protocol: algoritmo empleado por el protocolo WPA para mejorar la encriptación de los datos en redes wireless. Sus principales características son la renovación automática de la clave de encriptación de los mensajes y un vector de inicialización de 48 bits, lo que elimina el problema del protocolo WEP.

UNII (Unlicensed National Information Infraestructura): banda de frecuencia en los 5 GHz reservada por la FCC para las comunicaciones wireless según el estándar 802.11a. No existe una regularización internacional común sobre los aspectos de esta banda y los dispositivos que operan en ella.

WEP, Wired Equivalent Privacy: algoritmo de seguridad, de uso opcional, definido en el estándar 802.11. Basado en el algoritmo criptográfico RC4, utiliza una clave simétrica que debe configurarse en todos los equipos que participan en la red. Emplea claves de 40 y 104 bits, con un vector de inicialización de 24 bits.
Se ha demostrado su vulnerabilidad y que su clave es fácilmente obtenible con software de libre distribución a partir de cierta cantidad de tráfico recogido de la red.

Wi-Fi, Wireless Fidelity: nombre dado al protocolo 802.11b. Los dispositivos certificados como Wi-Fi son interoperables entre sí, como garantía para el usuario.

Wi-Fi Alliance, también llamada Wireless Ethernet Compability Alliance (WECA): asociación internacional formada en 1999 para certificar la interoperatibilidad de los dispositivos wireless basados en el estándar 802.11, con el objetivo de promover la utilización de dicha tecnología.

WPA, Wi-Fi Protected Access: protocolo de seguridad desarrollado por la WECA para mejorar la seguridad de la información en las redes wireless y permitir la autentificación de usuario, puntos débiles del WEP.

TITULO
DISEÑO RED INALÁMBRICA PAUs TRANSMILENIO S.A.

LADYS GISSELA OSPINO OROZCO [**]

Palabras claves: *802.11, Acces Point, Cifrado, PoE, WEP, filtrado de direcciones MAC, WDS.*

Resumen: este documento presenta el diseño de una red inalámbrica para la conexión entre los PAUs y la Sede Administrativa de Transmilenio S.A. Este diseño permite brindar al ciudadano un servicio personalizado en donde se podrá suministrar información sobre la operación del sistema y además se podrán presentar quejas y sugerencias por parte del usuario.
En este trabajo se podrán ver las fases que se llevaron a cabo antes de implementar la solución.

Inicialmente se evaluaron los requerimientos del cliente con el fin de ofrecer la mejor solución de acuerdo a lo que se desea, después se analizaron los estándares WI-FI existentes para escoger el más indicado para la solución, se revisaron varias opciones de seguridad y también se escogió que marca era la más indicada para esta solución teniendo en cuenta factores tales como Costo-Beneficio.

Por último se muestra el diseño final que fue presentado a Transmilenio S.A. el cual fue el escogido para implementar la solución y por medio de fotografías se da a conocer el montaje de este diseño, también se muestran gráficas en las cuales se puede ver claramente la configuración realizada a los Access Point y los pasos a seguir para configurar de forma correcta un acces point. Además se dan una serie de recomendaciones que hay que tener en cuenta para el montaje de la solución inalámbrica los cuales pueden ser de vital importancia.
Es de tener en cuenta que la característica más importante en este trabajo es el factor de Costo-Beneficio ya que con este se tomaron todas las decisiones finales para escoger los equipos.

---

[*] Trabajo de Grado

[**] Facultad de Ingenierías Fisicomecánicas, Escuela de Ingenierías Eléctrica, Electrónica y de Telecomunicaciones. Director: Jorge H. Ramón S. Magíster.

TITLE
WIRELESS NETWORK DESIGN
PAUs TRANSMILENIO S.A.[1]

LADYS GISSELA OSPINO OROZCO **

Key words*: 802.11, Acces Point, Encryption, PoE, WEP, filtrate of directions MAC, WDS.*

This document shows the wireless network design for connection between the PAUs and the administrative seat of Transmilenio S.A. . This design may offer the citizen a customized service where the information will be able to be provided about system operation, moreover, complaints and suggestions will be able to be presented on the part of the users.
In this work can be seen the phases that were carried out before implementing the solution.

Initially the requirements of client were evaluated with the purpose of offering the best solution according to which it is desired and then existing Wi-Fi standards were analyzed to select the most indicated for the solution; several security options we reviewed and also the mark that was most indicated for this solution was chosen considering factors such as cost- benefit.

Lastly, it shows the final design that was presented by Transmilenio S.A. which it was chosen to implement the solution and through photographies are released the assembly of this design, graphs are showed as well which it is possible to see clearly the configuration made to access point. Furthermore, a series of recommendations occurs that there is to consider for the assembly of the wireless solution which can be of vital importance.
It is to consider that the most important characteristic in this work is the factor of Cost-Benefit since with this all the final decisions were taken to choose the equipment.

---

* Thesis project

** Faculty of Physic-Mechanical Engineering , School of Electrical, Electronic and Telecommunications Engineering. Director: Oscar Gualdrón González, PhD.

INTRODUCCIÓN

El Sistema TransMilenio es un sistema de transporte masivo, que responde a las necesidades del transporte público en la ciudad de Bogotá. Ha construido una imagen de nueva ciudad como ejemplo nacional e internacional, la cual es reconocida y aceptada por todos los ciudadanos de Bogotá D.C. al prestar un servicio de transporte rápido, eficiente y seguro.

Esta imagen debe ser soportada y mantenida por todo el recurso humano que hace parte del Sistema de transporte y particularmente de TRANSMILENIO S.A. Es también evidente que la fortaleza tecnológica en que se soporta la operación y administración del sistema de transporte debe evolucionar hacia la satisfacción de los requerimientos de los usuarios.

Es por esto que Transmilenio S.A. creó los Puntos de Atención al Usuario que tienen como objetivo brindarle al ciudadano un servicio personalizado en donde puede encontrar toda la información sobre la operación del sistema y puede presentar quejas y sugerencias sobre el servicio.

Transmilenio S.A. busca contar con un diseño estructural abierto a la participación y construcción del diálogo permanente con sus usuarios, teniendo en cuenta que este sistema se encuentra en constante crecimiento y evolución.
De ahí la importancia de lograr un acercamiento oportuno, eficaz y ágil en los procesos de información y comunicación con los usuarios.
En la actualidad los usuarios cuentan con 5 mecanismos para establecer comunicación con Transmilenio y según estadísticas del sistema estas son las proporciones:

- Por escrito (carta o fax): 770 solicitudes (3.2 %).
- Línea 195: 11.589 Solicitudes (47.4 %).
- Correo electrónico (www.transmilenio.com): 9.376 solicitudes (38.4 %).
- Buzones: 2.033 solicitudes (8.3 %).
- Feria de servicio al ciudadano (realizada cada 15 días en diferentes localidades): 662 solicitudes (2.7 %).

Para un total de 24430 solicitudes.

Debido a la cantidad de solicitudes que se presentan en Transmilenio es necesario implementar un nuevo sistema de atención al usuario en el cual se pueda proporcionar de forma rápida y efectiva toda la información, reclamos y sugerencias que el usuario quiera comunicar.

Con los PAUs Transmilenio S.A. espera dar solución a los requerimientos de los usuarios con respuestas acertadas y efectivas en el menor tiempo posible.

Buscar una solución inalámbrica para dar una conexión rápida y eficiente entre el PAU y la sede administrativa de cada uno de sus portales es una necesidad para ofrecer el mejor servicio a sus usuarios.

LA EMPRESA

TechLAN Solutions es una compañía que entiende los objetivos del negocio de cada uno de sus clientes, ofreciendo servicios de soporte a nivel profesional en sectores de mayor crecimiento, incluyendo Tecnología LAN, Tecnología Inalámbrica, Seguridad, y Telefonía en Red, siendo lideres en Servicios profesionales de Networking, diseñando soluciones que involucran tecnología de punta con una excelente relación costo / beneficio, ofreciendo a sus clientes opciones de mantenimiento con tiempo de respuesta tales como soporte telefónico, paquetes de servicio 7x24, no incluidos en la garantía del producto.

Fuente: TechLAN Solutions Ltda. Documentos Internos.

SOLUCIONES WIRELESS

Diseño, configuración e implementación.

Los servicios profesionales de implementación de soluciones basadas en estándares inalámbricas que permiten plantear la mejor solución de acceso inalámbrico tanto a nivel LAN como soluciones de campus o interbuilding cumpliendo con los siguientes objetivos:

- Implementar de manera costo/beneficio la mejor solución.
- Diseñar soluciones que habiliten un alto desempeño en áreas de cubrimiento y servicios de LAN.
- Verificar conectividad en todos los usuarios con ubicación y flexibilidad.
- Crear controles de acceso para usuarios privilegiados e invitados.
- Establecer políticas basados en estándares de seguridad.
- Ahorrar dinero en cables costosos y difíciles de instalar.

RESULTADOS.

- Comunicación confiable bajo el principio de encriptación.
- Flexibilidad y movilidad para los usuarios de la red.
- Disminución de costos de implementación.
- Comunicación de dos o más sedes remotas sin tener que depender de un proveedor de servicios.
- No tener que hacer adecuación o reconstrucción de áreas para tener acceso a la red LAN.
- Transmisión con altos niveles de velocidad que ningún proveedor puede alcanzar sin un alto costo de servicio mensual.
- Disminución de costos.

1.0 REQUERIMIENTOS SOLUCIÓN INALÁMBRICA PAUs TRANSMILENIO S.A.

En las visitas realizadas a Transmilenio S.A. con los ingenieros del área de sistemas se analizaron los distintos requerimientos que se tendrían en cuenta para el diseño. En estas visitas se observaron los puntos en los cuales se ubicarían los PAUs y la distancia que estos tendrían a la sede administrativa de cada uno de los portales; la distancia medida entre el PAU y la Sede Administrativa fue de 58 metros. Por la ubicación de estos se llegó a la conclusión que la mejor alternativa era la de establecer una conexión inalámbrica ya que los PAUs están separados de la sede administrativa por el camino de desplazamiento de los buses alimentadores y por el camino de desplazamiento de los buses articulados de Transmilenio, como se puede observar en las siguientes gráficas.

Figura 1. Distancia del PAU a la Sede Administrativa en Portal Norte.

Fuente: autora del Proyecto.

Figura 2. Distancia del PAU a la Sede Administrativa en Portal de la 80.

Fuente: autora del proyecto.

Además otras de las razones por las cuales se llego a optar por una solución inalámbrica fue por los costos que significaba realizar una conexión por medio guiado, es decir por medio de cableado estructurado, debido a que esta implementación era muy alta respecto a la conexión inalámbrica. Para realizar estas conexiones se requería levantar las placas del camino de desplazamiento de los buses articulados, es decir levantar la plataforma, lo cual conllevaba a altos costos ocasionados por la mano de obra necesaria para realizar estas reformas, además de perjudicar gravemente el funcionamiento del portal. La otra alternativa para realizar la conexión entre el PAU y la Sede Administrativa era realizar un cableado aéreo, pero esto también fue descartado por los mismos ingenieros de Transmilenio. La principal razón por la cual se descarto esta solución fue por que las políticas de Transmilenio no permiten ningún tipo de cableado aéreo que

atraviese las vías de desplazamiento de los buses articulados o alimentadores dentro de los portales. Por estas razones ya mencionadas se toma la decisión de diseñar una solución inalámbrica.

Teniendo en cuenta que la mejor solución era la conexión inalámbrica el paso a seguir fue evaluar todos los requerimientos para buscar la mejor solución. En primera instancia el principal requerimiento era diseñar una red inalámbrica con alta velocidad y alta seguridad. Para cumplir con estos requerimientos se llevaron a cabo varias fases en las cuales se evaluaron todas las alternativas que existen tanto en el campo de estándares comerciales como en los de seguridad, además también se analizaron las marcas que fueron escogidas previamente por los ingenieros de Transmilenio para seleccionar la que mejor cumpliera con los requerimientos y que además tuviera mejor relación Costo-Beneficio.

Reuniendo todos los factores importantes de cada una de las reuniones realizadas en Transmilenio S.A. los requerimientos principales para esta solución fueron los siguientes:

- Lograr establecer una conexión inalámbrica entre el PAU y la Sede Administrativa. Esta deberá conectar un equipo de cómputo al switch principal que se encuentra ubicado en la Sede Administrativa.
- La conexión debe tener como mínimo una velocidad de 54 Mbps.
- Se debe tener en cuenta el crecimiento a futuro de Transmilenio en cada uno de sus portales, es decir la posibilidad de conectar más puntos a la Sede Administrativa.
- La cobertura de la antena utilizada para esta solución debe garantizar la conexión desde cualquier punto del portal a la Sede Administrativa siempre y cuando se pueda establecer una línea de vista hacia esta antena.
- La solución debe garantizar el correcto funcionamiento de la conexión inalámbrica, sin presentar ningún tipo de problemas por caída de la señal o por baja intensidad de la señal.

- La solución deberá brindar la posibilidad de enviar y recibir información desde el PAU hasta la Sede Administrativa y viceversa.
- Se debe implementar por lo menos un sistema de seguridad para prevenir la entrada de atacantes o personas no autorizadas que puedan ingresar a la red de Transmilenio S.A. Este se escogerá en común acuerdo con los ingenieros del área de sistemas de Transmilenio S.A.
- Considerando que el tráfico de datos será relativamente bajo (alrededor del 9% del tráfico total del portal) se implementará una solución que a futuro pueda soportar un aumento de tráfico en la red inalámbrica garantizando su correcto funcionamiento.

Teniendo en cuenta estos requerimientos las fases a seguir en este proyecto fueron:

- Análisis de estándares WIFI.
- Análisis de estándares de seguridad a manejar en WIFI.
- Evaluación de equipos a utilizar.

Para el desarrollo de estas fases se tomaron en cuenta los pros y los contras de cada estándar para luego escoger el que mejor cumplía con los requerimientos.
Teniendo cuenta estos puntos a continuación se muestra información más detallada de estos estándares y los factores que se tuvieron en cuenta para escoger la solución.

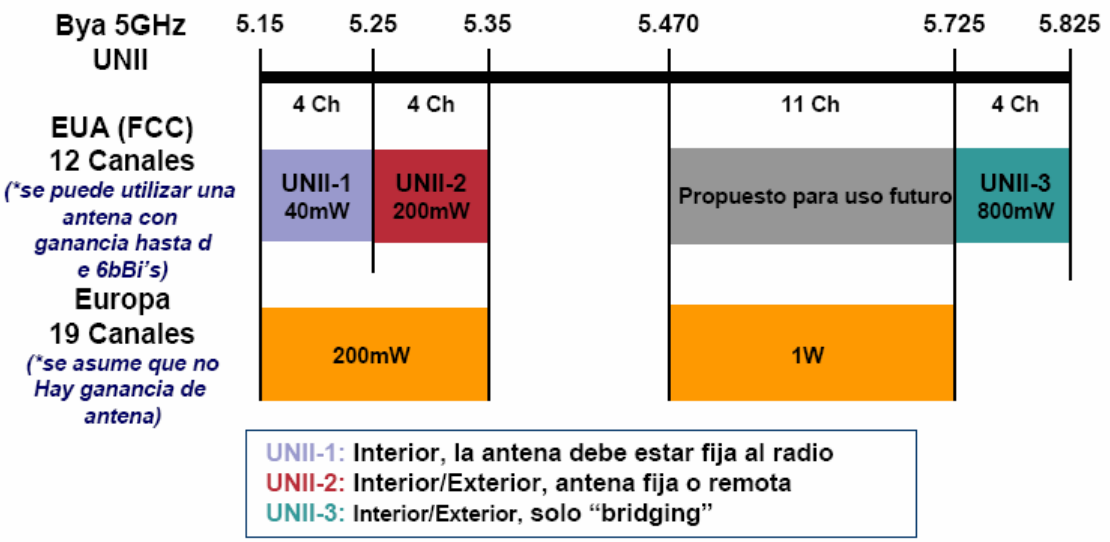
2.0 ANÁLISIS DE ESTÁNDARES COMERCIALES WIFI.

Los estándares comerciales WIFI más conocidos en el momento son el 802.11a, el 802.11b y el 802.11g.
Partiendo de estos se evaluaron sus pros y sus contras, teniendo en cuenta factores tales como velocidad, cobertura y compatibilidad con otros estándares.

El estándar 802.11a tiene muchas ventajas, entre estas su velocidad, ya que la velocidad máxima de este estándar es de 54 Mbps, esta velocidad es posible de alcanzar en distancias cortas, pero esta velocidad disminuye rápidamente a medida que tiene que atravesar paredes y otros obstáculos.
Otra de sus ventajas es la banda que utiliza, ya que este estándar trabaja en la banda de los 5 GHz, la cual es una banda que ofrece más canales y es menos utilizada que la banda de los 2.4 GHz. La banda de 5 GHz es una banda UNII (*Unlicensed National Information Infrastructure*) que emplea modulación OFDM (*Orthogonal Frequency Division Multiplexing*).
La banda UNII proporciona 300 MHz de espectro de frecuencia. Estos 300 MHz están divididos en dos segmentos: uno de 200 MHz que va desde 5.15 GHz hasta 5.35 GHz y otro de 100 MHz que va desde 5.725 GHz hasta 5.785 GHz.

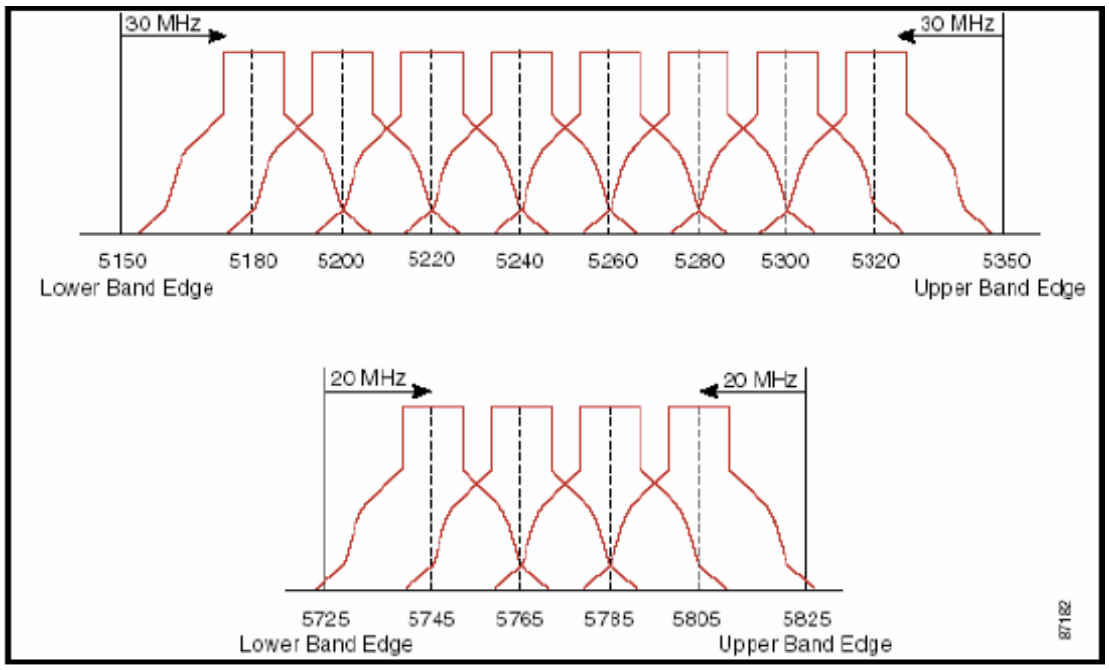
En la Figura No 3 se puede observar el espectro de frecuencia de la banda UNII de 5 GHz.

Figura 3. Espectro de 5 GHz



Fuente: Cisco Systems. Seminario de Redes Wireless LAN, Abril 2004. Disponible en internet: <URL: http:// www.cisco.com/global/MX/SemTecRouting/3_pres_**seminario**_tecnologico_seguridad_basico.pdf >.

Figura 4. Canales de la banda de 5 GHz



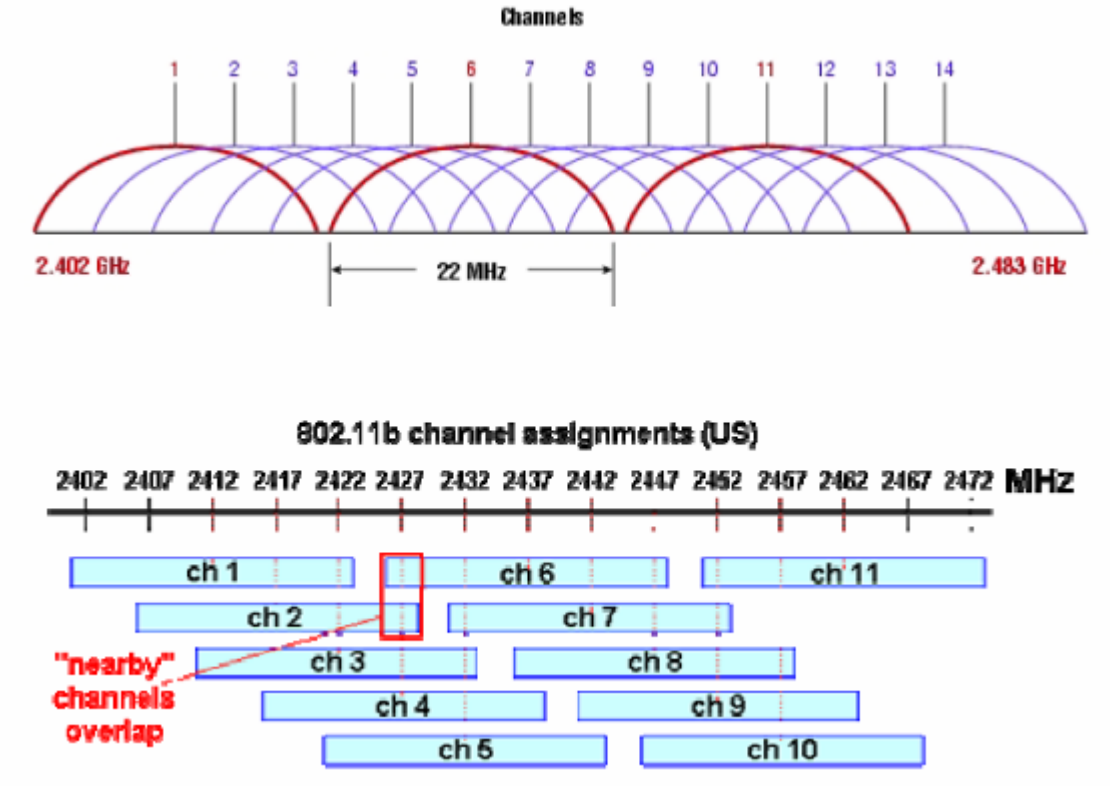
Fuente: Ph.D. Barradello, Carlos. Introducción a las Redes Wi-Fi: *Los Estándares Técnicos 802.11 b/g/a*, Volumen 1 Número 2, Noviembre 2003. Disponible en internet: <URL:http://www.icamericas.net/Cases_Reports/Wi-FiBriefs/WiFi2_Spanish.pdf>.

En la Figura No 4 se puede observar que la banda UNII de 5 GHz tiene 12 canales sin solapamiento o sobreposición.
Esta banda de 5 GHz es inmune a la interferencia de los equipos que trabajan en la banda de 2.4 GHz, tales como hornos microondas, teléfonos inalámbricos, Bluetooth y redes WiFi que operan en la banda de 2.4 GHz.

Pero a pesar de estas ventajas también tiene una desventaja, la cual es su incompatibilidad con los otros estándares, ya que la frecuencia que maneja este estándar es diferente a la frecuencia de los estándares 802.11b y g, y a pesar que estas dos bandas no tienen ninguna interferencia entre si, por estar en dos bandas de frecuencia diferentes los equipos de estos dos estándares no pueden comunicarse entre si. Otra de sus desventajas es la cobertura ya que este estándar tiene un alcance limitado de 50 metros, y con este alcance sería necesario montar más puntos de acceso de acuerdo a la distancia que se quiera cubrir, lo cual aumentaría los costos de implementación, eso sin mencionar que los equipos de este estándar son más costosos. En definitiva sus dos grandes desventajas son el rango de señal y sus costos los cuales pueden llegar a ser más altos que en la implementación de los otros estándares.

El estándar 802.11b opera en la banda ISM (*Industrial Scientific Medical*) y emplea una modulación DSSS (*Direct Sequence Spread Spectrum*). Tiene como primera desventaja su velocidad, ya que su máxima velocidad es de 11 Mbps la cual es mucho menor que el estándar 802.11a. El estándar 802.11b trabaja en la banda de 2.4 GHz que es una banda muy utilizada por teléfonos inalámbricos, hornos microondas y dispositivos Bluetooth, lo cual se considera como una desventaja ya que los equipos que operan en esta banda pueden causar interferencia. Otra desventaja que tiene el estándar 802.11b con respecto al 802.11a es la cantidad de canales, ya que el estándar 802.11b solo tiene 3 canales sin solapamiento, mientras que el 802.11a tiene 12 canales. En la figura No 5 podremos ver los canales del estándar 802.11b.

Figura 5. Asignación canales estándar 802.11b



Fuente: Rodriguez Orviz, Isabel y Vilas Paz, Manuel. Introducción a las tecnologías inalámbricas WiFi, Septiembre 2004. Disponible en internet: <URL:http://www.it.uniovi.es/material/cursos/**wifi**_COIIPA/Introduccion_802.11.pdf>.

Una ventaja que vale la pena resaltar es que el estándar 802.11b tiene un alcance de 100 metros el cual es mucho mayor al del estándar 802.11a que solo tiene un alcance de 50 metros, además el costo de implementación es más bajo ya que necesita menos puntos de acceso.

El estándar 802.11g permite una velocidad de transmisión de datos de 54 Mbps la cual iguala la velocidad del estándar 802.11a. Tiene la ventaja de que es compatible con el estándar 802.11b y además su cobertura es de 100 metros. Este estándar trabaja con dos tipos de modulaciones que son DSSS y OFDM. Con la modulación DSSS alcanza velocidades de hasta 11 Mbps y para velocidades

más altas utiliza la modulación OFDM que es la misma modulación que utiliza el estándar 802.11a.

El hecho de ser compatible con el estándar 802.11b es una gran ventaja ya que puede funcionar con equipos de este estándar a velocidades de 11 Mbps. Si se necesita velocidades más altas de hasta 54 Mbps es necesario que tanto las tarjetas de red como los puntos de acceso sean compatibles con el estándar 802.11g. A pesar de tener una velocidad igual al estándar 802.11a el estándar 802.11g no tiene el mismo ancho de banda de este. Al trabajar en la banda de 2.4 GHz tiene las mismas limitaciones que el estándar 802.11b, las cuales son un ancho de banda de 83.5 MHz el cual es casi 4 veces menor al del 802.11a y además solo tiene 3 canales que no presentan solapamiento o sobreposición. A la hora de nombrar las desventajas de este estándar se puede ver que son similares a la del estándar 802.11b, esto se debe a que estos dos estándares trabajan en la misma banda ISM de 2.4 GHz y por lo tanto tiene la misma desventaja en cuanto a interferencia se refiere, pero también tiene la ventaja de que su cobertura máxima es de 100 metros.

Se puede decir que este estándar reúne las mejores características de los otros dos estándares, las cuales son mejor cobertura, mejor velocidad y menor costo de implementación.

Al revisar todas estas características de cada uno de los estándares junto con los ingenieros de Transmilenio S.A. se tomó la decisión de tomar el estándar 802.11g como el estándar adecuado para esta solución. La razón principal por la cual se escogió fue por su buena relación costo-beneficio, ya que los equipos de este estándar ofrecen muchas ventajas tales como buena cobertura, buen precio y velocidades de transmisión altas, además también es un estándar compatible con el 802.11b.

Aunque el estándar 802.11a también ofrecía muchas ventajas, la razón por la cual no se adoptó fue debido a su baja cobertura, ya que en la evolución de

Transmilenio S.A. está implementar en un futuro otros puntos de atención y para esto se requiere una tecnología que ofrezca la suficiente cobertura como para comunicar cualquier punto de los portales a sus respectivas sedes administrativas.

A continuación se presenta un cuadro comparativo de los 3 estándares mencionados.

Tabla 1: Estándares WIFI

ESTANDAR	VENTAJA	DESVENTAJA	PRECIOS APROXIMADOS
802.11a	Ofrece velocidades de hasta 54 Mbps. Opera en la banda de 5 GHz que es una banda menos congestionada y con menor interferencia.	Ofrece tan solo un alcance de 50 metros. La banda de 5 GHz ofrece menor cubrimiento y además los equipos que trabajan con este estándar son menos populares.	2.000.000
802.11b	Tiene un alcance de hasta 100 metros.	Solo ofrece una velocidad máxima de 11 Mbps. Trabaja en la banda de 2.4 GHz que es la misma banda donde trabajan los teléfonos inalámbricos y los hornos microondas.	900.000

802.11g	Su alcance es de 100 metros. Su velocidad máxima es 54 Mbps. Compatible con el estándar 802.11b.	Trabaja en la banda de 2.4 GHz que es la misma banda donde trabajan los teléfonos inalámbricos y los hornos microondas.	1.100.000

Nota: los precios varían de acuerdo a la marca, y en algunos casos las marcas ofrecen equipos que trabajan con los 3 estándares.

3.0 ANÁLISIS DE ESTÁNDARES DE SEGURIDAD EN WIFI

En la historia de la comunicación inalámbrica uno de los puntos más importantes siempre ha sido la seguridad.

Hasta el momento se han creado muchos métodos de seguridad en WIFI, unos con más seguridad que otros. A continuación se nombraran algunos de los estándares de seguridad en WIFI y se resaltaran sus pros y sus contras.

El algoritmo WEP se diseñó con el fin de proporcionar confidencialidad, autentificación y control de acceso a las redes WIFI. WEP trabaja a nivel de capa 2 del modelo OSI y es un cifrado que es soportado por la mayoría de fabricantes de soluciones Wireless.

WEP utiliza una clave simétrica y estática en las estaciones y en el punto de acceso. El algoritmo de cifrado utilizado es RC4 con claves de 64 bits. Los 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta que es la que se distribuye manualmente. El vector de inicialización (IV) es generado dinámicamente y debe ser diferente para cada trama. Lo que se busca con el IV es cifrar con claves diferentes cada trama para así evitar que alguien pueda capturar suficiente tráfico cifrado con la misma clave y al final logre deducirla.

El algoritmo de cifrado WEP funciona de la siguiente manera:

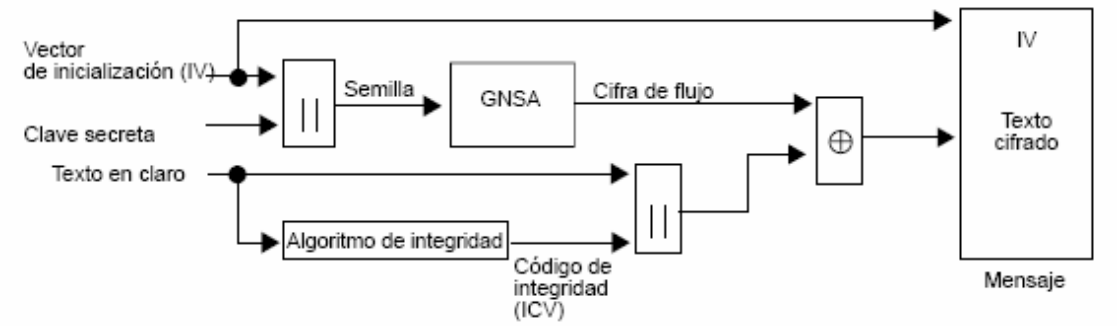
A la trama se le computa un código de integridad (Integrity Check Value, ICV) mediante el algoritmo CRC-32. Este ICV se concatena con la trama y se emplea más tarde por el receptor para comprobar si la trama ha sido alterada durante el transporte.

Se escoge una clave secreta entre el emisor y el receptor la cual puede tener 40 o 128 bits. Para evitar tramas cifradas similares se concatena la clave secreta con un número aleatorio al cual se le llama vector de inicialización (IV), este número cambia en cada trama.

La concatenación de la clave secreta y el IV (también conocida como semilla) se emplea como entrada de un generador RC4 de números pseudo-aleatorios.

El generador RC4 genera una cifra de flujo de mismo tamaño de la trama a cifrar más 32 bits, estos 32 bits son para cubrir la longitud de la trama y el ICV. Luego se hace un XOR bit por bit de la trama con la secuencia de la clave obteniéndose como resultado la trama cifrada. El IV y la trama se transmiten juntos.

Figura 6. Funcionamiento del algoritmo WEP en modalidad de cifrado



Fuente: Madrid Molina, Juan Manuel. Seguridad en redes inalámbricas 802.11, Abril 2004. Disponible en internet: <URL:http://www.icesi.edu.co/.../publicaciones/contenidos/sistemas_telematica/3/jamdrid-seguridad_redes_inalambricas.pdf>.

A pesar que el algoritmo WEP resuelve el problema de cifrado de datos entre emisor y receptor hay situaciones que hacen a este algoritmo inseguro.

En la mayoría de instalaciones se emplea el algoritmo WEP con claves de cifrado estáticas, además estas claves se cambian pocas veces o nunca. Esto hace la tarea más fácil para un atacante que quiera obtener la clave de acceso a la red inalámbrica, ya que puede acumular grandes cantidades de texto cifrado para así obtener la clave.

Otro de los problemas que presenta el cifrado WEP es que el IV tiene una longitud de tan solo 24 bits, por lo tanto es cuestión de tiempo para que se agote el espacio de 2^{24} IV distintos, esto en una red de alto tráfico puede pasar en tan solo 5 horas. Si el atacante logra obtener dos tramas con IV idénticos entonces puede obtener la clave secreta, para esto ya existen una serie de programas en la web con los cuales obtener esta clave sería relativamente sencillo. Entre estos se encuentra Aircrack la cual contiene tres utilidades principales.

La primera detectar redes que tengan activado WEP como protocolo de seguridad, la segunda incrementar el tráfico en la red con esta seguridad y la tercera descifrar la clave WEP cuando logra obtener dos IVs iguales.

Otra herramienta utilizada es la llamada Chopchop cuya funcionalidad es descifrar paquetes cifrados con WEP sin conocer la clave.

Al igual que estos hay otros que trabajan de maneras similares y que también son posibles de conseguir en la web.

WEP también tiene el problema de no ofrecer el servicio de autenticación, por lo tanto el cliente no puede autenticar la red ni la red puede autenticar al usuario. Por esto para que la comunicación pueda llevarse a cabo sólo se necesita que el equipo y el punto de acceso compartan la clave WEP.

El WPA es un estándar que busca solucionar los problemas de WEP, mejorando el cifrado y ofreciendo un servicio de autenticación. Las principales características de WPA son la distribución dinámica de claves, mejor utilización del IV y nuevas técnicas de autenticación.

Para lograr todo esto WPA propone un nuevo protocolo de cifrado conocido como TKIP (Temporary Key Integrity Protocol). Este protocolo se encarga de cambiar la clave compartida ente el punto de acceso y el cliente cada cierto tiempo. El mecanismo de autenticación usado en WPA emplea 802.1x y EAP.

WPA puede operar en dos modalidades las cuales son modalidad de red empresarial y modalidad de red casera.

Para operar en la modalidad de red empresarial es necesario un servidor RADIUS en la red. El punto de acceso utiliza 802.1x y EAP para la autenticación y el servidor RADIUS provee las claves compartidas para cifrar los datos.
Para una red casera también llamada PSK (Pre-Shared Key) sólo se necesita introducir una contraseña compartida entre el punto de acceso y los equipos. Cuando ya se logra el acceso TKIP entra en funcionamiento, con esto se garantiza la seguridad. Una de las recomendaciones para este estándar es emplear contraseñas de 20 o más caracteres ya que se a comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta.

WPA soluciona la debilidad del IV de WEP aumentando el tamaño del vector a 48 bits, con esto se aumenta la cantidad de combinaciones de claves diferentes, es decir aumentan a 2^{48}. El algoritmo utilizado para WPA sigue siendo RC4, y el CRC-32 fue cambiado por el MIC. Con WPA se evita la modificación manual de las claves ya que estas son generadas dinámicamente y distribuidas de forma automática.

WPA2 o estándar 802.11i es el nuevo estándar del IEEE para proporcionar seguridad en redes WIFI. WPA2 incluye un nuevo algoritmo de cifrado AES (Advanced Encryption Standard), este es un algoritmo de cifrado de bloque con claves de 128 bits.
La nueva arquitectura que utiliza el WPA2 para las redes WIFI se llama RSN (Robust Security Network) y utiliza autenticación 802.1x, distribución de claves robustas y nuevos mecanismos de integridad y privacidad.
Para asegurar la autenticidad e integridad de los mensajes WPA2 utiliza CCMP (Counter-Mode / Cipher Block Chaining / Message Authentication Code Protocol) en lugar de MIC.
Los métodos de autenticación soportados son 802.1x y PSK (Pre-Shared Key).
Los protocolos de seguridad utilizados para el tráfico unicast y multicast son CCMP y TKIP. Además este estándar ofrece soporte para la pre-autenticación

cuya funcionalidad es permitir a los usuarios pre-autenticarse antes de cambiar de punto de acceso en la misma red.

La autenticación 802.1x es basada en EAP y en el método específico de autenticación decidido. Entre estos esta EAP/TLS con certificados de cliente y servidor (requiere una infraestructura de claves públicas), y EAP/TTLS o PEAP para autenticación híbrida (con certificados sólo requeridos para servidores).
Un punto importante de WPA2 es la seguridad que utiliza en las claves ya que cada clave tiene un tiempo de vida determinado y la seguridad global se garantiza utilizando un conjunto de varias claves organizadas según la jerarquía, de esto se trata el RSN.
Cuando ya se ha establecido el contexto de seguridad y al obtener una autenticación exitosa, se crean claves temporales de sesión y se actualizan con regularidad hasta que se cierra el contexto de seguridad.
Este estándar de seguridad es el más robusto hasta el momento y la única debilidad conocida hasta el momento es en el ataque contra la clave PSK, ya que puede ser sometido a ataques de diccionario. Esta debilidad se puede eliminar escogiendo una clave que no sea una frase que este en el diccionario y que preferiblemente tenga 20 o más caracteres. Otra desventaja que vale la pena nombrar es el tiempo de duración de la autenticación, ya que en algunas ocasiones puede llegar a ser un poco molesto debido a la demora de este, esto es muy incomodo para usuarios que requieren autenticarse con mucha frecuencia debido a que mantienen en constante desplazamiento de su puesto de trabajo a otros puntos y se puede perder tiempo valioso mientras se espera a ser autenticado. Esto depende de la capacidad del equipo utilizado, ya que debe tener un buen soporte de RSN para evitar estos inconvenientes.

El filtrado de direcciones MAC consiste en crear una tabla de datos en cada uno de los puntos de acceso de la red inalámbrica. Esta tabla debe contener las direcciones MAC (Media Acces Control) de las tarjetas de la red inalámbrica que

se pueden conectar al punto de acceso. Como ya se sabe toda tarjeta de red posee una dirección MAC única, con esta MAC se logra autenticar el equipo.
Este mecanismo tiene como principal desventaja el no poseer ningún mecanismo de cifrado, por lo tanto las direcciones MAC y todos los datos viajan sin cifrar. Si un atacante capturara este tráfico, podría capturar las direcciones MAC de tarjetas matriculadas en la red y podría asignarle una de estas direcciones a la tarjeta de su equipo. Esto es posible por medio de programas que se consiguen fácilmente en la web. Entre estos se pueden mencionar el AirJack6 o WellenReiter.

Otra de sus desventajas ocurre cuando en la red hay muchos equipos, entonces el trabajo de crear la tabla de datos con todas las MAC se hace tediosa.
Es importante tener en cuenta que con este método no se garantiza la confidencialidad de la información transmitida ya que no ofrece ningún mecanismo de cifrado como se dijo anteriormente.

Teniendo en cuenta estas características de algunos de los métodos de seguridad en WIFI, se presentó un informe a los ingenieros de Transmilenio S.A. en los cuales se aconsejaba implementar como método de seguridad el estándar WPA. Los ingenieros de Transmilenio manifestaron el interés de escoger WEP como el estándar de seguridad a utilizar para la solución, esto debido a que las tarjetas de red de algunos equipos de Transmilenio no soportan el estándar WPA, y estos equipos están proyectados a futuro. TechLAN Solutions Ltda. en vista de la decisión tomada por Transmilenio y previendo los problemas que podría acarrear utilizar WEP como estándar de seguridad aconsejó utilizar además de este estándar el método de seguridad de filtrado de direcciones MAC, para darle otro nivel de seguridad a la solución.

4.0 EQUIPOS DE RED EVALUADOS PARA LA SOLUCIÓN INALÁMBRICA

En mutuo acuerdo con el área de sistemas de Transmilenio S.A. las marcas escogidas para analizar fueron 3Com, Cisco y Allied Telesyn.
Las razones por las cuales se prefirieron estas marcas fueron por ser muy conocidas tanto por Transmilenio S.A. como por TechLAN Solutions Ltda. Estas marcas ya han sido utilizadas anteriormente por TechLAN Solutions Ltda. y se han obtenido excelentes resultados en todas las soluciones implementadas, además Transmilenio S.A. ya conocía la marca 3Com que fue utilizada en una solución anterior y con la cual tuvieron muy buenos resultados.

Como primer paso se entraran a evaluar los puntos de acceso (Acces Point) de cada una de las marcas mencionadas anteriormente. Después se evaluaron las antenas a utilizar para la solución teniendo en cuenta los factores que pueden afectar la comunicación para escoger la potencia más adecuada de las antenas.

A continuación se mostraran los Acces Point escogidos para evaluar de acuerdo a cada una de las marcas mencionadas anteriormente.

3Com Acces Point 8750.

Este Acces Point de 3Com es ideal para crear LAN inalámbricas de clase empresarial, ofrece un alto rendimiento ya que soporta hasta 253 usuarios simultáneos. Este Acces Point tiene un punto de acceso bi-direccional, es decir maneja los estándares 802.11a y 802.11g y soporta transmisiones de radio de 5 GHz y 2.4 GHz.

El Acces Point 8750 ofrece Clear Channel Select que es una herramienta que escoge el canal menos traficado, y con esto ofrece conexiones sin ningún tipo de problema.

Otro punto importante es que este Acces Point soporta PoE, esto es una gran ventaja ya que este Acces Point puede recibir datos y alimentación a través de un mismo cable, esto se logra adquiriendo el respectivo adaptador Power Over Ethernet.

Ofrece cifrado WEP de clave compartida de 40/64 bits y 128/54 bits, y también ofrece cifrado WPA AES de 256 bits.

La autenticación 802.1x del servidor RADIUS controla el acceso a la red inalámbrica y centraliza la autorización de los usuarios en toda la red.

Tiene la opción de administración dinámica de claves de sesión y asignación de claves dinámicas por medio de TKIP lo que ofrece una mejor seguridad.

Entre otras opciones de seguridad también tiene control de acceso de direcciones MAC por medio del filtrado de MAC.

A continuación se muestran las especificaciones técnicas de este equipo.

Tabla 2. Especificaciones técnicas 3Com Acces Point 8750

Especificaciones Técnicas.	
Usuarios Soportados	Hasta 253 usuarios simultáneos
Cumplimiento con estándares	Certificación Wi-Fi, IEEE 802.11a, IEEE 802.11g
Velocidades de datos	802.11a: 54, 48, 36, 24, 18, 12, 9, 6Mbps (hasta 108 Mbps en modalidad turbo) 802.11g: 54, 48, 36, 24, 18, 11, 9, 5.5, 2, 1 Mbps
Banda de frecuencia	802.11a: 5 GHz 802.11g: 2.4 GHz
Medio inalámbrico	802.11a: OFDM, 802.11g: OFDM y DSSS (con

	codificación Barker y CCK para compatibilidad con el estándar anterior 802.11b)
Protocol de Acceso de Medios	CSMA/CA
Canales operativos	802.11a: 36 - 64 (total de 8) 802.11g: 1 - 11 (EUA y Canadá), 1 - 13 (en todo el mundo; la disponibilidad del canal depende de regulaciones locales)
Alcance operativo	802.11a: hasta 50 metros (164 pies) de transmisión y recepción 802.11g: hasta 100 metros (328 pies) de transmisión y recepción
Configuraciones de potencia de transmisión	802.11a: 17 dBm en banda baja dependiendo de la velocidad en bits; 20dBm en banda media dependiendo de la velocidad en bits; 802.11g: 17 dBm dependiendo de la velocidad en bits
Seguridad	Encriptación WEP de 40/64 y 128/154 bits; encriptación WPA AES de 256 bits, encriptación Dynamic Security Link de 128 bits; 802.11x con autentificación de servidor RADIUS; autentificación EAP-MD5, EAP-TLS, EAP-TTLS y PEAP; ESSID broadcast control, autentificación MAC local; listas de control de acceso a servidores, administración de Sesiones Dinámicas de Claves y TKIP, asignación dinámica VLAN, filtración cliente a cliente y uplink
Gestión de red	Herramienta para "Site survey", Wireless Infrastructure Device Manager, Wireless LAN Discovery Tool, 3NS, SNMP

Fuente: 3Com. Disponible en internet:

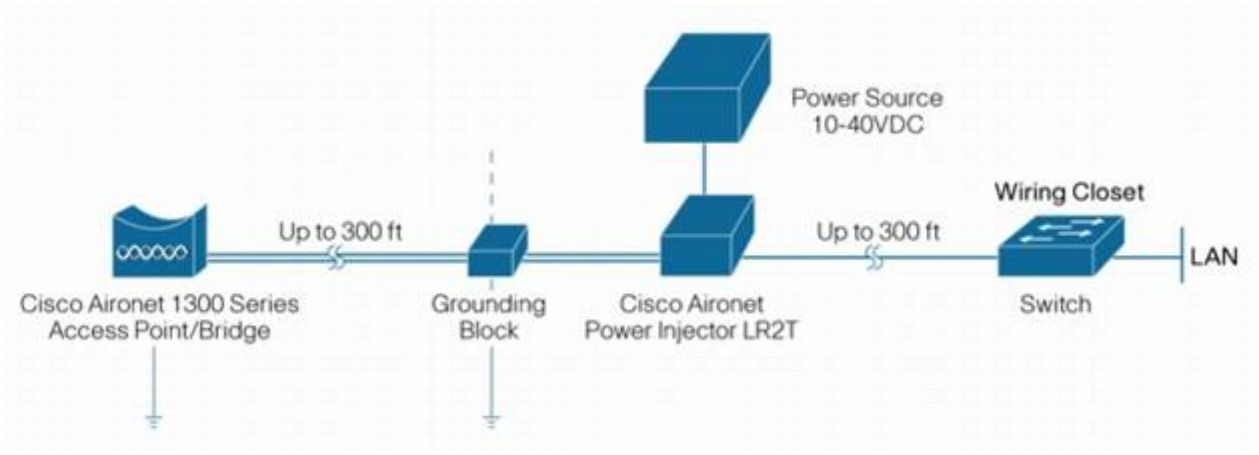
<URL: http://www.3com.com/prod/es_LA_AMER/detail.jsp?tab=prodspec&sku=3CRWE875075A>.

Cisco Aironet 1300 Series Outdoor Access Point/Bridge.

El Cisco Aironet 1300 Series Outdoor Access Point/Bridge es un punto de acceso 802.11g y bridge que proporciona alta velocidad y conectividad wireless rentable entre redes fijas o móviles y entre clientes.
Este Acces Point soporta el estándar 802.11g y provee una velocidad de 54 Mbps y mantiene la compatibilidad con equipos del estándar 802.11b.

Este equipo soporta los estándares de seguridad WPA y WPA2 y numerosos tipos de protocolos de autenticación extensible (EAP). También soporta el IEEE 802.1x para uso basado en la autenticación, TKIP para cifrado WPA y AES para WPA2.
Tiene la ventaja de poder ser configurado como Acces Point, Bridge o Workgroup bridge. Soporta configuraciones punto a punto o punto-multipunto. Otra gran ventaja es que su chasis esta diseñado para entornos de intemperie con un rango de temperaturas muy alto.
El cisco Aironet 1300 también viene con un Power Injector, este convierte el estándar 10/100BASET a una interfaz coaxial que es más conveniente para ambientes al aire libre.
A continuación se mostrara un diagrama en el que se podrá ver la conexión de la red con el Power Injector.

Figura 7. Diagrama de red con el Power Injector



Fuente: Cisco Systems. Disponible en internet:
<URL: http://www.cisco.com/en/US/products/ps5861/products_data_sheet09186a00802252e1.html>.

A continuación se mostrara una tabla con las características principales del Cisco Aironet 1300.

Tabla 3. Especificaciones técnicas Cisco Aironet 1300.

Estándares	IEEE 802.11b or IEEE 802.11g
Bandas de Frecuencia	· 2.412 a 2.462 GHz (FCC) · 2.412 a 2.472 GHz (ETSI) · 2.412 a 2.472 GHz (TELEC)
Modulación	802.11b · Direct Sequence Spread Spectrum (DSSS): · Differential Binary Phase Shift Keying (DBPSK) a 1 Mbps · Differential Quadrature Phase Shift Keying (DQPSK) a 2 Mbps · Complementary Code Keying (CCK) a 5.5 y 11 Mbps 802.11g · Orthogonal Frequency Divisional Multiplexing (OFDM): · BPSK a 6 y 9 Mbps · QPSK a 12 y 18 Mbps

	· 16-quadrature amplitude modulation (QAM) a 24 y 36 Mbps · 64-QAM a 48 y 54 Mbps
Protocolo de Acceso al Medio	CSMA/CA
Canales de Operación	802.11b/g · ETSI: 13 · America: 11 · TELEC (Japon): 13
Canales sin solapamiento	3
Seguridad	Cisco Wireless Security soporta WPA y WPA2, esto incluye la protección contra paquetes maliciosos y contra intrusos que quieran entrar a la red. Si un Acces Point detecta un ataque malicioso se genera una alarma por los puntos de acceso pertenecientes a la red y este es enviado al controlador Cisco Wireless LAN y con esto se evita la entrada de intrusos en la red. El soporte 802.1X incluye EAP con ciertos de sus métodos tales como EAP-TLS, EAP-TTLS y PEAP que son algunos métodos de autenticación. El cifrado utilizado en el Cisco Aironet 1300 es TKIP y MIC para WPA y AES para WPA2.
SNMP	Versión 1 y 2

Fuente: Cisco Systems.

Allied Telesyn Enterprise-class Wireless Access Point.
AT-WA7400

El AT-WA7400 es un Acces Point que opera en las dos frecuencias que son 2.4 GHz y 5 GHz. Soporta los estándares 802.11a, b y g.

Este Acces Point esta equipado con estándares de cifrado y autenticación tales como WPA/WPA2, WEP, TKIP, cifrado AES/CCMP, filtrado de direcciones MAC y control de acceso por vía Radius con EAP y PEAP.

Ofrece velocidades de hasta 54 Mbps utilizando los estándares 802.11a y 802.11g.

Asegura la red Wireless dividiendo el acceso en segmentos públicos y privados con BSSIDs múltiples, direcciones MAC y VLAN Tagging.

La detección de Acces Point maliciosos proporciona la capacidad de detectar y localizar puntos de acceso no autorizados y así previene la entrada no autorizada a la red Wireless.

El AT-WA7400 ofrece un avanzado balance de cargas que permite balancear la distribución de las conexiones Wireless de los clientes a través de los múltiples Acces Point mejorando el rendimiento y la utilización del ancho de banda.

Otra de sus grandes ventajas es que puede soportar Power Over Ethernet que es tan importante cuando se necesita montar equipos que no están cerca de una fuente de poder y que no están cerca del sitio donde se producen los datos.

A continuación se muestran las características principales del AT-WA7400.

Tabla 4. Especificaciones técnicas AT-WA7400

Administración	- Web - Telnet/CLI - SNMP v1 and v2 - Standard 802.11 MIB and ATI-private MIB (based on draft 802.11k)

	- Network Time Protocol (NTP)
Estándares	802.11a, 802.11b y 802.11g
Asignación de IP	- DHCP - Static IP
Seguridad	El AT-WA7400 soporta Filtrado de MAC hasta para 256 entradas, también soporta 802.1X, WEP con llaves de 64, 128 y 152 bits, WPA incluyendo TKIP, EAP y PSK, WPA2 con todo el soporte de 802.11i. También detecta Access Point no autorizados y envía una alarma al Allied Telesyn Wireless Network Manager y evita la entrada de clientes no autorizados.
SNMP	Version 1 y 2
Protocolo de red y compatibilidad de los estándares	IEEE802.3 CSMA/CD IEEE802.3u 100BaseTX IEEE802.11g IEEE 802.11i IEEE802.1x Draft IEEE 802.11f Draft IEEE 802.11e
PoE	- Proporciona energía por el mismo cable de datos. - Facilita la instalación de un Acces Point donde no se tiene una toma de corriente cercana.
WDS	Es útil cuando se requiere extender una red y los costos por cableado son costosos. Permite la comunicación directa con otros Access Point tanto en modo bridge como en modo repetidor.

Fuente: Allied Telesyn

A continuación se mostrara un cuadro comparativo de las marcas escogidas.

Tabla 5. Cuadro comparativo marcas 3Com, Cisco y Allied Telesyn.

	3Com	Cisco	Allied Telesyn
Estándares	802.11a y 802.11g	802.11b y 802.11g	802.11a, 802.11b y 802.11g
Banda(s) de Frecuencia	802.11a: 5 GHz 802.11g: 2.4 GHz	2.412 to 2.462 GHz (FCC)	802.11a: 5 GHz 802.11b y g: 2.4 GHz
Modulación	802.11a: OFDM, 802.11g: OFDM y DSSS	802.11b: DSSS 802.11g: OFDM	802.11a: OFDM, 802.11b: DSSS, 802.11g: OFDM y DSSS
Seguridad	WEP; WPA AES de 256 bits; 802.11x con autentificación de servidor RADIUS; autentificación EAP-MD5, EAP-TLS, EAP-TTLS y PEAP; ESSID broadcast control, autentificación MAC local; listas de control de acceso a servidores, administración de Sesiones Dinámicas de Claves y TKIP, asignación dinámica VLAN	Cisco Wireless Security soporta WPA y WPA2, esto incluye la protección contra paquetes maliciosos y contra intrusos que quieran entrar a la red. Si un acces point detecta un ataque malicioso se genera una alarma por los puntos de acceso pertenecientes a la red y este es enviado a el controlador Cisco Wireless LAN y con esto se evita la entrada de intrusos en la red. El soporte 802.1X incluye EAP con ciertos de sus métodos tales como EAP-TLS, EAP-TTLS y PEAP que	El AT-WA7400 soporta Filtrado de MAC hasta para 256 entradas, también soporta 802.1X, WEP con llaves de 64, 128 y 152 bits, WPA incluyendo TKIP, EAP y PSK, WPA2 con todo el soporte de 802.11i. También detecta Access Point no autorizados y envía una alarma al Allied Telesyn Wireless Network Manager y evita la entrada de clientes no autorizados.

		son algunos métodos de autenticación. El cifrado utilizado en el Cisco Aironet 1300 es TKIP y MIC para WPA y AES para WPA2.	
PoE	Si	Si (Power Injector)	Si
WDS	Si	Si (LWAPP)	Si
Factor Costo-Beneficio	Es un equipo que cumple con los requerimientos, pero por experiencia se sabe que no se obtienen buenos resultados en soluciones Wireless implementadas con esta marca	Es un equipo robusto, de excelente calidad y con todos los requerimientos que se necesitan pero su principal desventaja es el precio y esto lo hace de difícil adquisición	Es un equipo robusto, cumple con todos los requerimientos y por experiencia se sabe que son equipos de excelente calidad y con excelentes resultados en soluciones Wireless, además son equipos de fácil adquisición por su bajo precio en comparación a las otras marcas
Precios	2.231.000	3.887.000	1.380.000

Fuentes: 3Com, Cisco Systems y Allied Telesyn.

En una reunión realizada con los Ingenieros del área de sistemas de Transmilenio S.A. se discutió que equipo escoger para esta solución y cual presentaba mejores características, además también se tuvo en cuenta cual presentaba mejor factor de Costo-Beneficio.

Se llego a la conclusión de que los 3 equipos escogidos para evaluar presentaban muy buenas características que se amoldaban perfectamente para esta solución, TechLAN Solutions Ltda. recomendó las marcas Cisco y Allied Telesyn ya que estas marcas fueron utilizadas anteriormente en otras soluciones y presentaron excelentes resultados, la marca 3Com fue descartada para esta solución por recomendación de TechLAN Solutions Ltda. debido a que con esta marca no se han tenido muy buenos resultados en soluciones Wireless implementadas anteriormente. Después de tomar la decisión de que las marcas más adecuadas para esta solución eran Cisco y Allied Telesyn se entró a evaluar cual de estas marcas era más asequible en cuanto a precio es decir cual presentaba mejor característica de Costo-Beneficio. Con este último factor de evaluación la marca descartada para la solución fue Cisco ya que esta marca si bien tiene equipos muy robustos también tiene precios muy altos. Por lo tanto, el equipo escogido para esta solución fue el AT-WA7400 de la marca Allied Telesyn, ya que esta marca no solo ofrece equipos robustos sino que también posee la mejor característica de Costo-Beneficio, esto sin nombrar los excelentes resultados que se han tenido en implementaciones anteriores.

Otro punto importante en esta solución es la selección de las antenas a utilizar. Para esto se tuvo en cuenta la distancia y el medio en el cual se iba a implementar la solución. Como ya se nombro antes, el PAU y la Sede Administrativa están separados por el camino de desplazamiento de los alimentadores y de los buses articulados de Transmilenio S.A. y por lo tanto este camino de comunicación que se establece entre el PAU y la Sede Administrativa esta expuesta a la intemperie. Debido a que la buena comunicación en camino depende de las condiciones climáticas tales como la lluvia y de las posibles interferencias que se puedan

presentar en los alrededores por otras redes Wireless o incluso por interferencia de otros equipos tales como teléfonos inalámbricos u hornos microondas, se pensó que la mejor forma de garantizar una buena comunicación entre estos dos puntos de Transmilenio era instalando antenas con muy buena potencia. Para escoger las antenas adecuadas se consultaron algunas marcas que ofrecen antenas en el mercado teniendo preferencia por las antenas QP-COM ya que esta marca ofrece antenas de alta potencia, de buena calidad y con excelente precio. TechLAN Solutions Ltda. ya ha trabajado en otras ocasiones con estas antenas, por esta razón las prefiere sobre otras marcas.

Se consultó con los Ingenieros del área de sistemas de Transmilenio S.A. la opción de implementar la solución con las antenas QP-COM y se presentaron las razones por la cual TechLAN Solutions Ltda. prefiere esta marca por sobre las otras. Las razones que TechLAN Solutions Ltda. presentó fueron las siguientes:

- Son antenas que ofrecen buena ganancia.
- Ya se han implementado anteriormente con buenos resultados.
- Ofrecen buena relación Costo-Beneficio.

Los Ingenieros del área de sistemas de Transmilenio S.A. estuvieron de acuerdo con las razones presentadas y por tal razón la marca escogida para las antenas fue QP-COM.

Debido a la distancia que ahí desde el PAU hasta el punto donde estarán ubicados el Acces Point y la Antena se tomo la decisión de utilizar un Power Over Ethernet para enviar la información y los datos hasta el Acces Point. Esta tecnología permite que los dispositivos Ethernet como por ejemplo los Acces Point reciban alimentación y datos a través de un mismo cable. Este estándar PoE también conocido como IEEE802.3af es el primer estándar internacional de distribución de alimentación a través de una LAN Ethernet. Entre sus ventajas están:

- Utilizar un único juego de cables para conectar el dispositivo Ethernet en este caso el Acces Point y suministrarle alimentación y datos.
- Los dispositivos se instalan fácilmente ya que lo único que se necesita es un cable LAN, y además evita el problema de no poder alimentar un equipo debido a que no hay una fuente de poder próxima al equipo.

Para esto se escogió el DWL-P100 de D-Link que es un adaptador Power Over Ethernet que suministra alimentación a otros periféricos utilizando el puerto Ethernet común. Esto es una buena solución para nuestro problema ya que el Acces Point no va a estar cerca del PAU y tampoco va a estar cerca de una toma eléctrica.

El DWL-P100 consiste en una unidad base y una unidad Terminal conectadas entre si a una distancia máxima de 100 metros, mediante un cable Ethernet estándar de categoría 5.

Su principal funcionalidad es suministrar alimentación (CC) a otros periféricos a través del puerto Ethernet utilizando cableado de categoría 5 y además transforma la entrada CA en corriente continua CC de bajo voltaje en salida. Pero su principal aplicación es el hecho de llevar energía y datos por un mismo el cual es el cable UTP de categoría 5.

A continuación se presentara la solución propuesta a Transmilenio S.A. para implementar una red inalámbrica entre los PAUs y las Sedes Administrativas de cada uno de los portales.

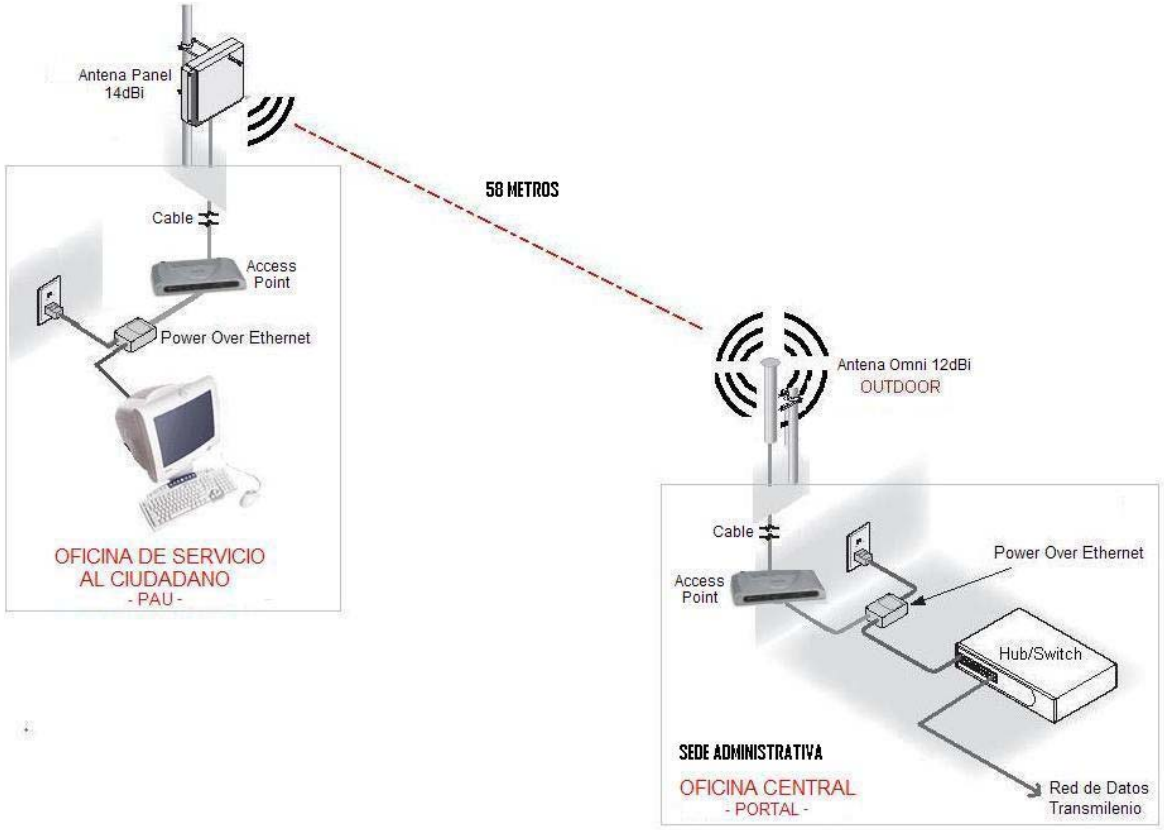
5.0 SOLUCIÓN PRESENTADA A TRANSMILENIO S.A

En la solución presentada a Transmilenio S.A. se planteo una solución inalámbrica con equipos Allied Telesyn, antenas QP-COM y adaptadores Power Over Ethernet D-Link, en donde se encuentran dos puntos de Acceso Inalámbrico conectados cada uno a una antena las cuales se ubicaron de tal forma que las dos tuvieran línea de vista con velocidad de conexión a 54 Mbps.

El esquema que se planteó comienza por la conexión del Power Over Ethernet, este se conecta a la toma de corriente y al cable de datos que viene del equipo de cómputo del PAU. De este sale un cable UTP hasta el Acces Point el cual se encarga de hacerle llegar los datos y la alimentación a este. Luego el Acces Point se conecta a la antena la cual es una antena panel que establece una conexión direccional y se encarga de enviar o radiar los datos. Del otro lado en la Sede Administrativa se encuentra una antena omnidireccional, esta antena se escogió omni pensando en el crecimiento de Transmilenio que a futuro puede crear más puntos lejanos a la Sede Administrativa que necesiten comunicación con ella. Esta antena recibe los datos que vienen desde la antena panel del PAU y se conecta al otro Acces Point que esta ubicado cerca de la Sede Administrativa y el cual se conecta por medio del cable UTP que viene del Power Over Ethernet el cual se encarga tanto de alimentarlo como de enviar o recibir datos de este Acces Point, este Power Over Ethernet va a la toma de corriente y el otro cable que sale del Power Over Ethernet que es un cable UTP va al Switch de la Sede Administrativa.

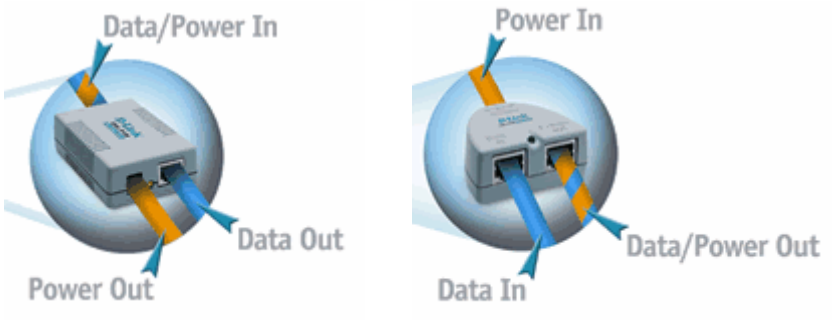
A continuación se mostrara un esquema en el cual se vera de forma más detallada la solución propuesta.

Figura 8. Esquema solución Inalámbrica PAU Transmilenio S.A



Fuente: TechLAN Solutions Ltda. Documentos Internos.

Figura 9. Dibujo detallado del DWL-P100



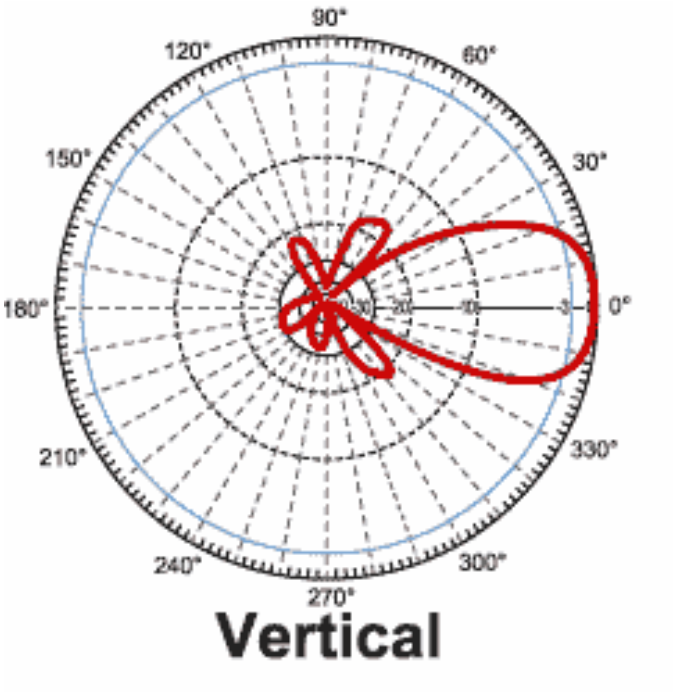
Fuente: wireless.uzice.net. Disponible en internet: <URL: http://wireless.uzice.net/uputstvo-poe-kako_ga_napraviti.htm>.

En la figura 9 se muestran los dos módulos del DWL-P100. El primer módulo recibe el cable de la toma eléctrica y el cable UTP de datos que viene del equipo de computo del PAU, por el otro lado del modulo sale un cable UTP el cual lleva los datos y la alimentación, este cable se conecta al Acces Point AT-WA 7400 y con esto el equipo queda en funcionamiento, es decir recibe los datos del PAU y la vez recibe alimentación. Del otro lado, en el Acces Point de la Sede Administrativa se utiliza este mismo modulo. El otro modulo no se usó porque no era necesario, ya que este Acces Point soportaba PoE, además se hizo una prueba en la cual se separo los datos y la energía con este modulo, y el resultado no fue muy satisfactorio, debido a que el Acces Point no funcionaba correctamente, el equipo no recibía la energía suficiente para funcionar adecuadamente y por esta razón el equipo no lograba arrancar.

La antena panel QP-COM escogida fue la QP-AO14P Antena de 2.4GHz, 14dBi, Flat Panel, ya que esta es la antena panel que ofrece más ganancia en la marca QP-COM. Esta es una antena plana direccional de alto rendimiento y trabaja en la banda de 2.4 GHz incluyendo los estándares 802.11b y g, Bluetooth y hotspots Wireless públicos. Esta antena es ligera y se puede instalar en polarización horizontal o vertical, puede ser montada en la pared o sobre el techo así como también se puede montar sobre un mástil.

A continuación se mostrara el patrón de ganancia de la antena QP-AO14P en polarización vertical.

Figura 10. Patrón de ganancia antena QP-AO14P en polarización vertical



Fuente: QP-COM. **Disponible en internet**:
<URL: http://qpcom.emultired.com/asp/producto.asp?lang=2&idproducto=72>.

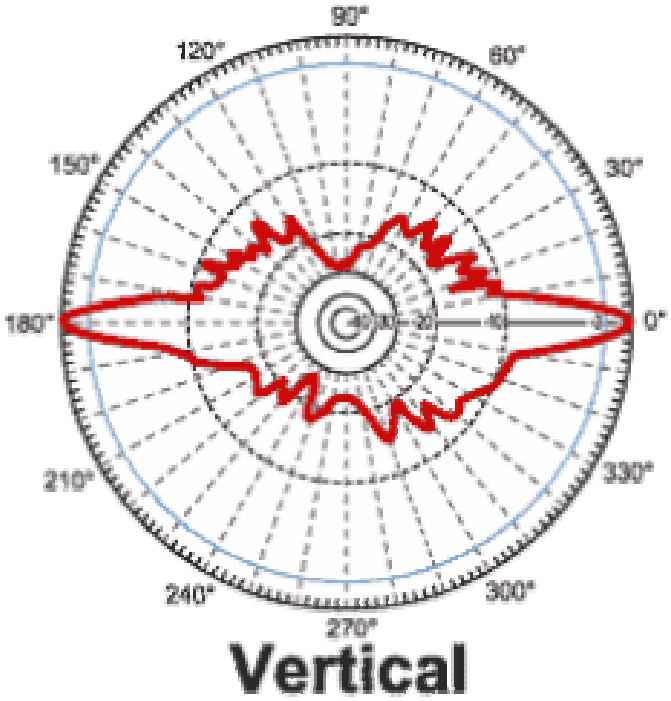
La antena omnidireccional escogida fue la QP-AO12O Antena 2.4GHz, 12dBi, OMNI Directional. Esta también se escogió por ser la antena omnidireccional QP-COM con mayor ganancia.

Trabaja en la frecuencia de 2.4 GHz y se usa para los estándares 802.11b y g, para Bluetooth y otras aplicaciones multipunto en donde se desea una cobertura amplia.

El sistema de montaje consiste en un soporte de acero y un par de pernos de 2.5 pulgadas.

A continuación se muestra el patrón de ganancia de la antena QP-AO12O en polarización vertical.

Figura 11. Patrón de ganancia antena QP-AO12O en polarización vertical



Fuente: QP-COM. **Disponible en internet**:
<URL: http://qpcom.emultired.com/asp/producto.asp?lang=2&idproducto=70>.

A continuación se muestran las tablas con los equipos utilizados en cada portal y el total de equipos de la solución.

Tabla 6. Total equipos inalámbricos necesarios para cada los portales

EQUIPO INALÁMBRICO	No. De Parte	CANTIDAD
Allied Telesyn Enterprise-class Wireless LAN Access Point	AT-WA7400	2
Antenna 2.4GHz, 12dBi, OMNI Directional	QP-AO120	1
Antenna 2.4GHz, 14dBi, Flat Panel	QP-AO14P	1
Cable SMA to N-Male connector 2mts	QP-ACRS2NM	2
Power Over Ethernet	DWL-P100	2

Fuente: TechLAN Solutions Ltda. Documentos Internos.

Tabla 7. Total equipos inalámbricos necesarios para todos los portales

EQUIPO INALÁMBRICO	No. De Parte	CANTIDAD
Allied Telesyn Enterprise-class Wireless LAN Access Point	AT-WA7400	8
Antenna 2.4GHz, 12dBi, OMNI Directional	QP-AO120	4
Antenna 2.4GHz, 14dBi, Flat Panel	QP-AO14P	4
Cable SMA to N-Male connector 2mts	QP-ACRS2NM	8
Power Over Ethernet	DWL-P100	8

Fuente: TechLAN Solutions Ltda. Documentos Internos.

Esta solución fue presentada al área de sistemas de Transmilenio S.A. para su aprobación. Los ingenieros estuvieron de acuerdo en la solución propuesta y el siguiente paso fue coordinar los últimos detalles de la solución en cada uno de los 4 portales de Transmilenio S.A.

6.0 DISEÑO FINAL RED INALÁMBRICA PAUs TRANSMILENIO S.A

El propósito de este diseño es proveer conectividad inalámbrica a una velocidad de 54 Mbps y con unos requerimientos de seguridad para convertir esta red en una red segura en cada uno de los portales que son Usme, Tunal, 80 y Norte.

Para esto se diseñó una solución inalámbrica con arquitectura completamente plana en la cual los equipos ya antes mencionados se ubican estratégicamente para obtener una línea de vista.

A continuación se mostraran las ubicaciones donde estos equipos fueron instalados.

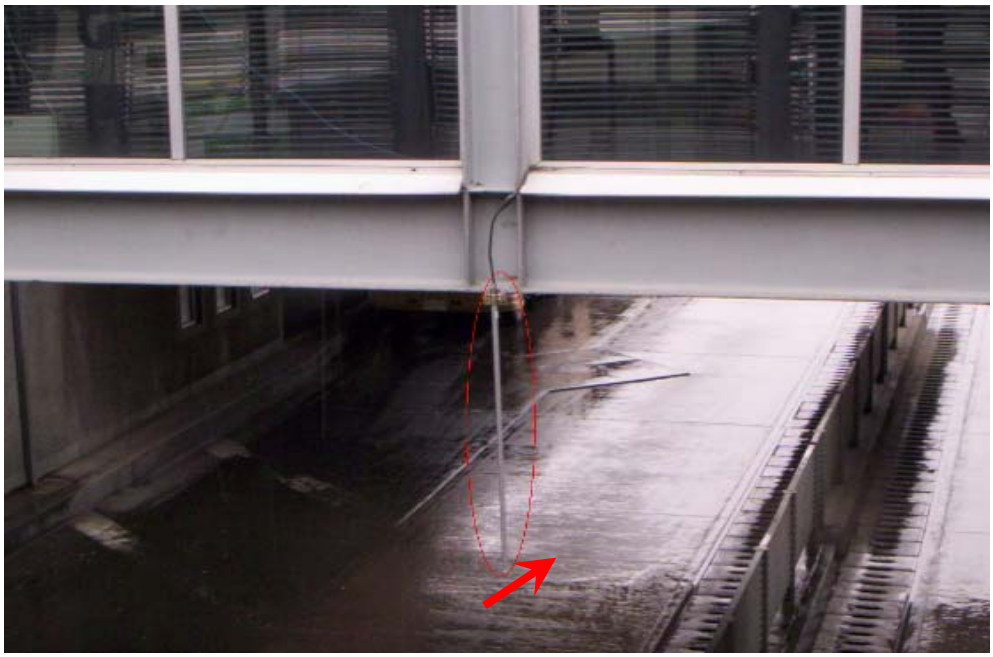
Figura 12. Antena Panel instalada en Portal Norte

Fuente: autora del proyecto.

Figura 13. Antena Panel instalada en Portal Norte (segunda vista)

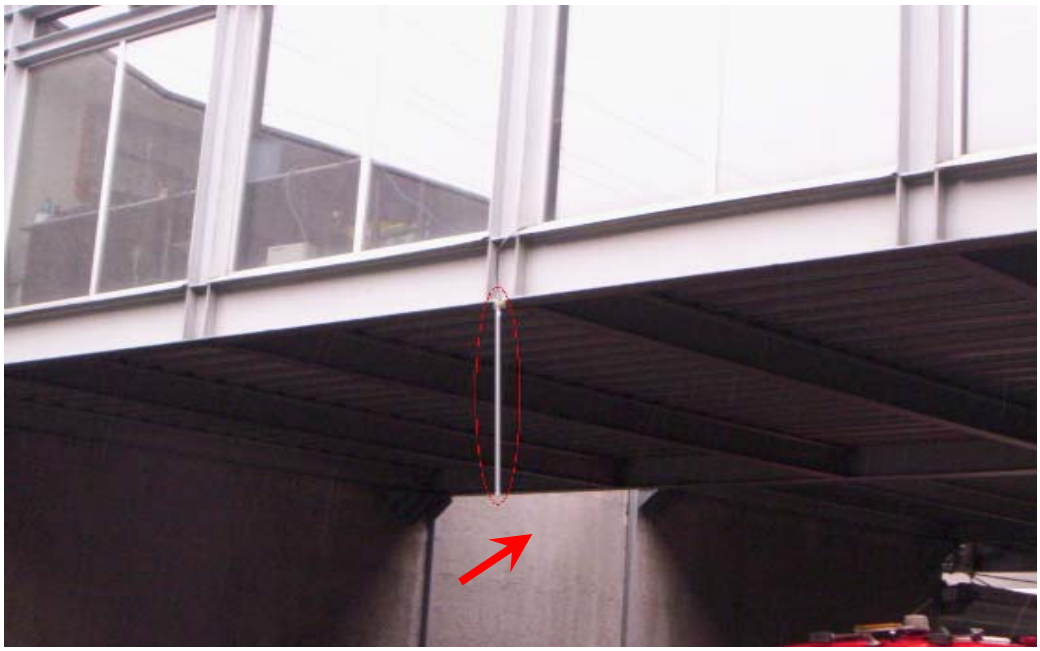
Fuente: autora del proyecto.

Figura 14. Antena Omni instalada en Portal Norte



Fuente: autora del proyecto.

Figura 15. Antena Omni instalada en Portal Norte (segunda vista)



Fuente: autora del proyecto.

Figura 16. Portal de la 80

Fuente: autora del proyecto.

Figura 17. Antena Panel instalada en Portal de la 80

Fuente: autora del proyecto.

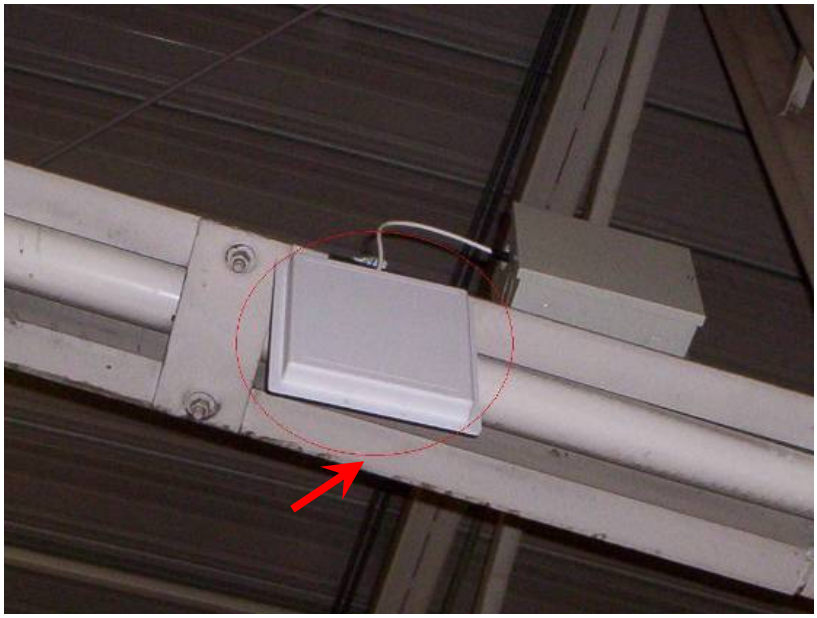
Figura 18. Acces Point 7400 de Allied Telesyn junto con el PoE de Dlink instalados en Portal de la 80

Fuente: autora del proyecto.

Figura 19. Antena Omni instalada en Portal de la 80

Fuente: autora del proyecto.

Figura 20. Antena Panel instalada en Portal del Tunal



Fuente: autora del proyecto.

Figura 21. Antena Panel instalada en Portal del Tunal (segunda vista)

Fuente: autora del proyecto.

Las imágenes de la antena Omni instalada en el Portal del Tunal y las antenas Panel y Omni instaladas en el portal de Usme no fueron posibles de tomar debido a la hora en la cual se realizó la instalación de todos los equipos de la solución.

Una vez instalados las antenas y los equipos en cada uno de los portales se proveyó a la configuración de los Acces Point.

Asignación de Direcciones IP

De común acuerdo con el Jefe de Sistemas de Transmilenio S.A. como representante del departamento de Sistemas de Transmilenio y evaluando las

ventajas que esto conlleva, se configuraron los Access Points con direcciones IP estáticas, de la siguiente forma:

Tabla 8. Direcciones IP asignadas en cada portal

PORTAL USME			
AP	MAC Access Point	IP	Ubicación
1	00:OC:46:F2:E5:08	192.168.0.50	OFICINA
2	00:OC:46:F2:E5:00	192.168.0.51	PAU

PORTAL TUNAL			
AP	MAC Access Point	IP	Ubicación
1	00:OC:46:F2:E4:F8	10.10.10.10	OFICINA
2	00:OC:46:F2:E5:20	10.10.10.11	PAU

PORTAL 80			
AP	MAC Access Point	IP	Ubicación
1	00:OC:46:F2:DF:AB	192.168.0.10	OFICINA
2	00:OC:46:F2:E4:E0	192.168.0.11	PAU

PORTAL NORTE			
AP	MAC Access Point	IP	Ubicación
1	00:OC:46:F2:E5:18	192.168.0.10	OFICINA
2	00:OC:46:F2:E4:E8	192.168.0.11	PAU

Fuente: autor del proyecto.

Nota:

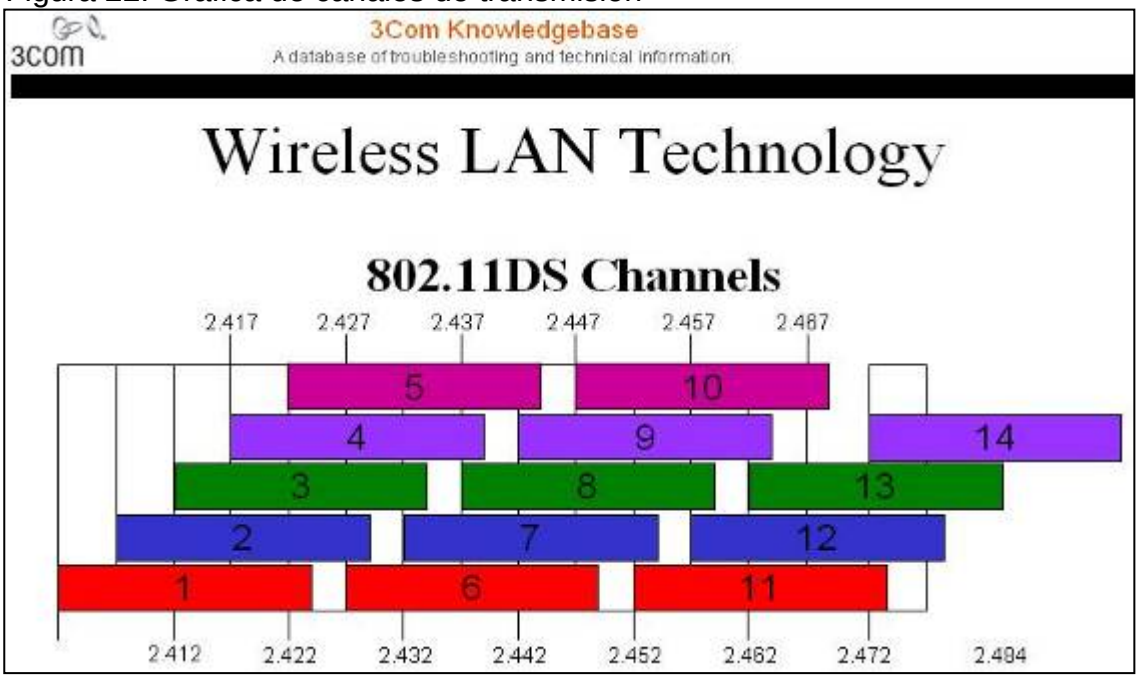
- Los Computadores de Escritorio ubicados en cada PAU obtendrán dirección IP automáticamente del Servidor DCHP del Cable MODEM del Proveedor de Servicio de Internet (ISP) ubicado en cada PAU.
- Las Mascaras de Subred utilizadas en la configuración son Tipo C (255.255.255.0)

Asignación de Canales de Transmisión

Se asignó como canal de Transmisión para cada Access Point (AP), el canal 8, con el objeto de eliminar cualquier tipo de Interferencia y saturación con otros APs aledaños o cercanos indiferentes a la red de datos de Transmilenio.

Esta asignación del canal de Transmisión se evaluó de acuerdo a la siguiente grafica.

Figura 22. Gráfica de canales de transmisión



Fuente: TechLAN Solutions Ltda. Documentos Internos.

Principales Características de la Configuración

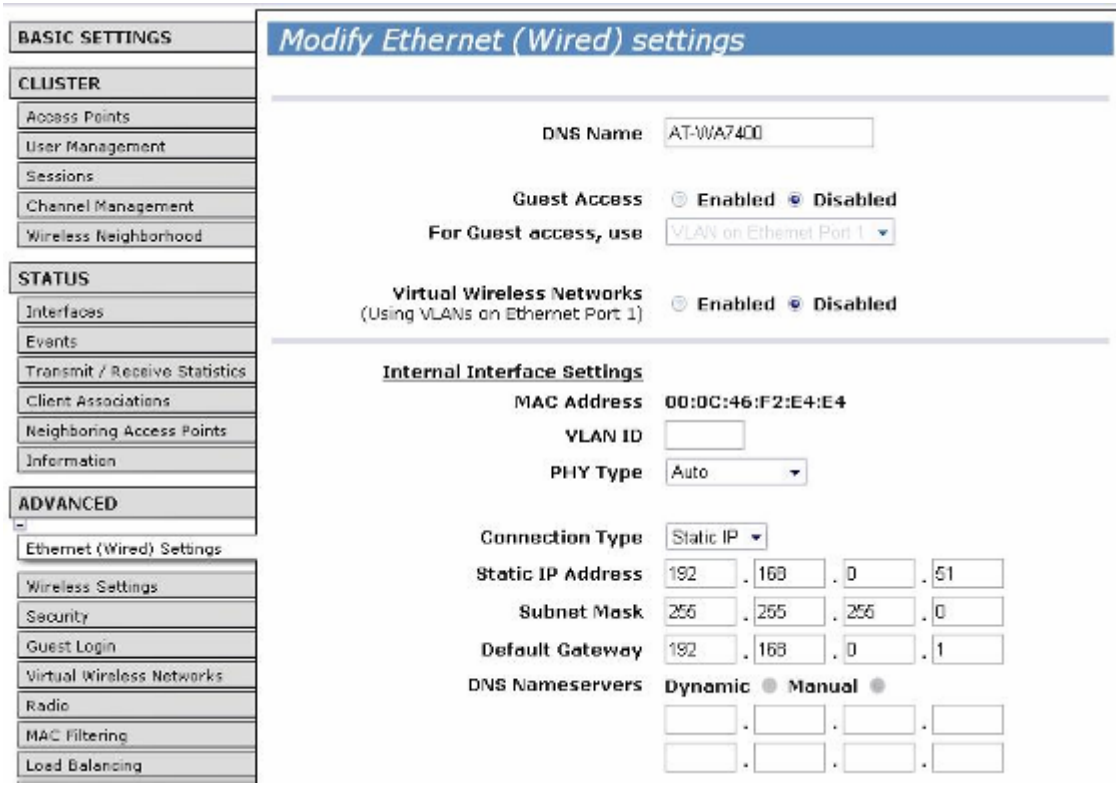
El Login y el Password asignados a los Acces Points fueron los indicados por los Ingenieros del área de sistemas de Transmilenio los cuales fueron los siguientes:

- Access Point System Login : PAU
- Access Point System Password : PAUTRANM

Una vez se entra al Acces Point se asigna la dirección IP estática, esta dirección se toma de la Tabla No mostrada anteriormente.

- Dirección IP : Static IP (ver asignación de direcciones IP)

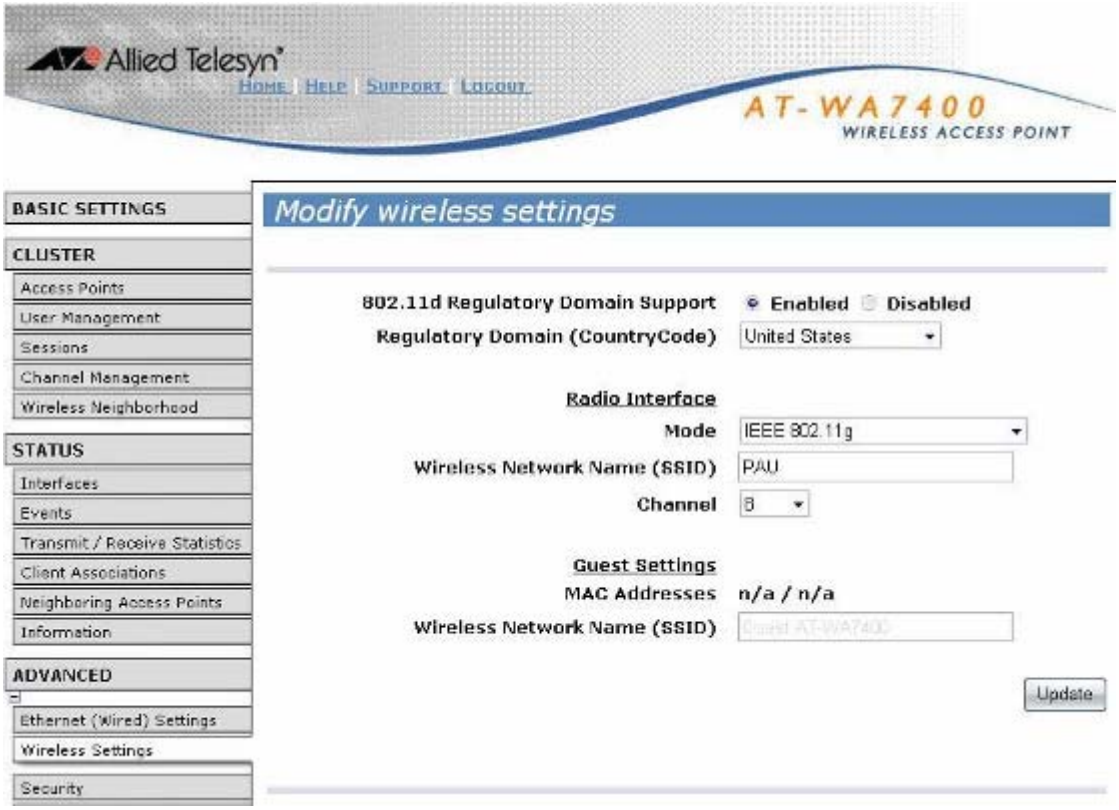
Figura 23. Print Screen de la asignación de dirección IP estática



Fuente: TechLAN Solutions Ltda. Documentos Internos.

En el esquema siguiente se muestra como se configura el modo de transmisión el cual en este caso es el estándar 802.11g, se configura el SSID o nombre de la red Wireless y se le asigna el canal de transmisión.

Figura 24. Print Screen del modo de configuración del estándar.

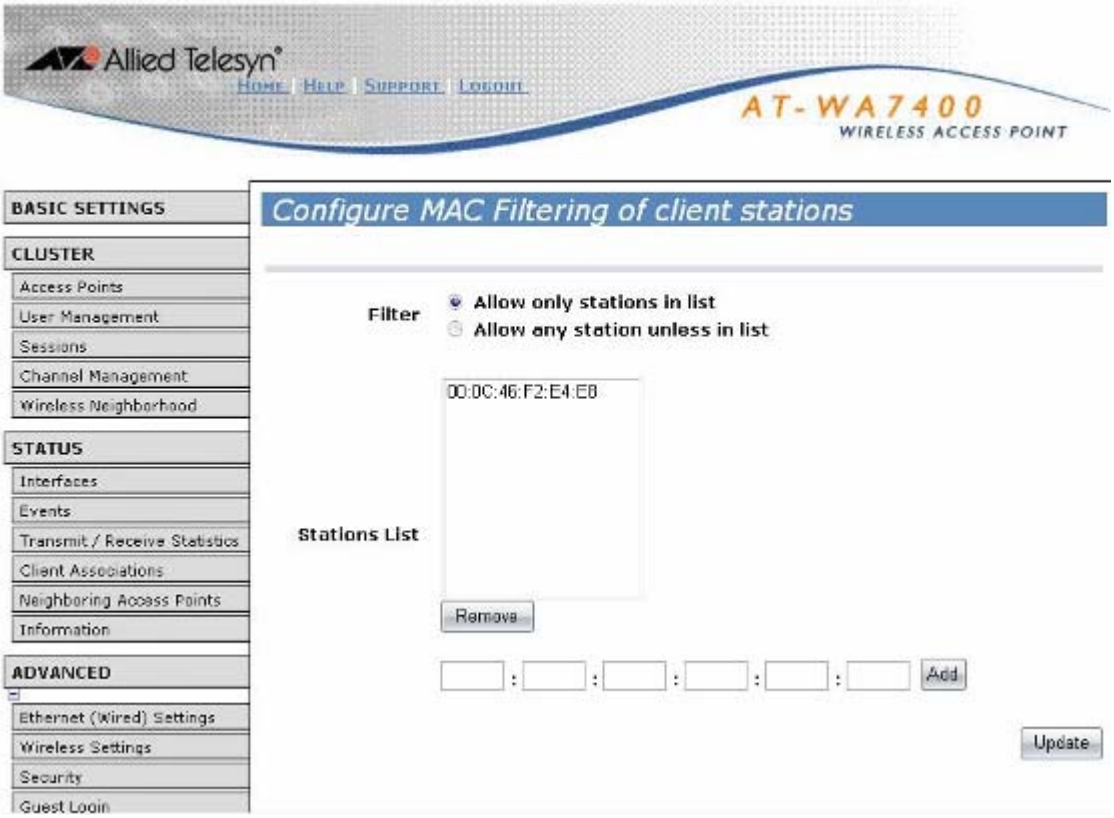


Fuente: TechLAN Solutions Ltda. Documentos Internos.

- Modo de Transmisión: IEEE 802.1g (54Mbps)
- SSID / Wireless Network Name: PAU
- Canal de Trasmisión: 8 (ver asignación de Canales de Transmisión)

El siguiente paso es la configuración del Filtrado de MAC

Figura 25. Print Screen de la configuración del Filtrado de MAC



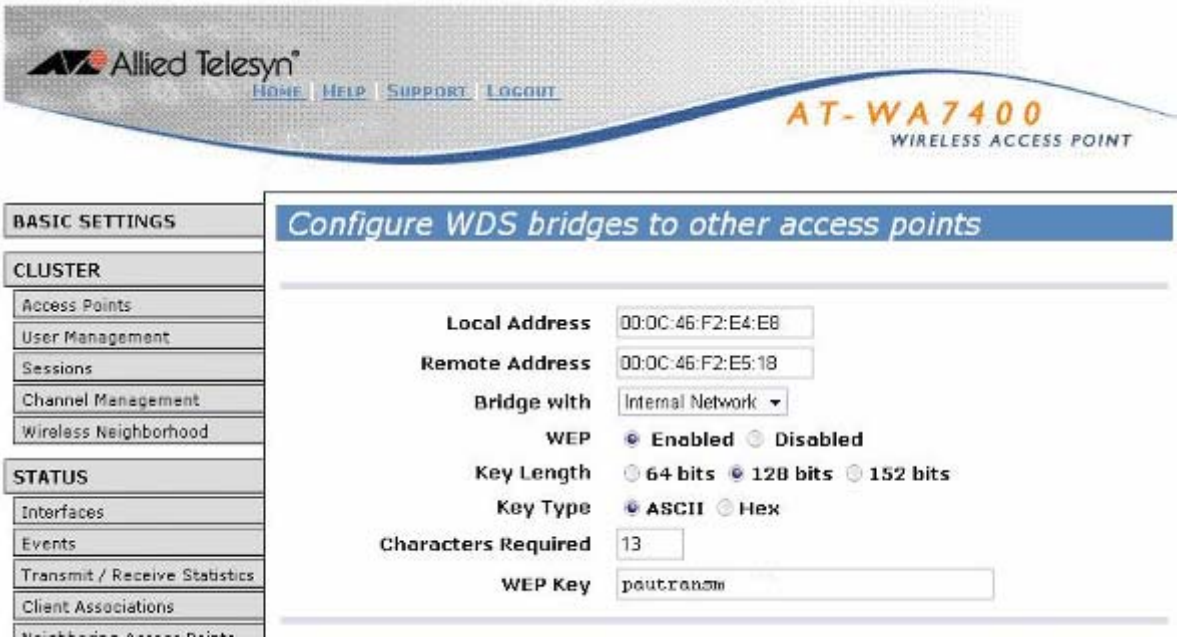
Fuente: TechLAN Solutions Ltda. Documentos Internos.

- MAC Filtering : Allow Only Stations in List

  Nota: Este Ítem es el que hace que el Enlace Inalámbrico montado en los PAUs de Transmilenio sea altamente seguro ya que los Access Point solo dejaran acceder a la red los equipos inalámbricos que estén configurados en esa lista y al que no se encuentren en esa lista no les dará por ningún motivo acceso a la red.

El siguiente paso es realizar la configuración del **WDS** (Wirelesss Distribution System) y del segundo nivel de seguridad. El WDS permite que dos o más Acces Point se interconecten de manera inalámbrica. En este caso se interconectara el Acces Point del PAU con el Acces Point de la Sede Administrativa.

Figura 26. Print Screen configuración WDS



Fuente: TechLAN Solutions Ltda. Documentos Internos.

- Local Address: MAC Access Point Local
  (Ver asignación de direcciones IP)
- Remote Address: MAC Access Point Remoto
  (Ver asignación de direcciones IP)
- Security: Enable

WEP

Mode: 128-bit encryption

Key: pautransm

Default Key ID: 2

Nota: Este Ítem le da a la solución inalámbrica montada un Segundo nivel de Seguridad ya que cifra la información transmitida con un algoritmo matemático de 128 Bits, así cualquier intruso que obtenga la información no la podrá entender ya que esta codificada y cifrada.

Por último se realizaron pruebas de conectividad y operatividad en cada uno de los PAUs de los portales Usme, Tunal, 80 y norte. Esto dio como resultado un correcto funcionamiento y total operatividad de acuerdo a los requerimientos y expectativas de Transmilenio S.A. Estas pruebas fueron corroboradas y evaluadas por el Ing. Jhon Alonso como representante del Departamento de Sistemas de Transmilenio a total satisfacción del mismo.

Las pruebas realizadas consistieron en enviar archivos desde el PAU hasta la Sede Administrativa, se probaron diferentes tamaños de archivos con un máximo tamaño de 5MB. Estos archivos llegaron de forma correcta, para el caso del archivo de 5 MB el tiempo de transferencia fue de 4 minutos a una velocidad aproximada de 15 KB/s.

7.0 CONCLUSIONES

Se presentó un diseño final en el cual se logra la conectividad inalámbrica de dos puntos de Transmilenio los cuales son el PAU y la Sede Administrativa de cada uno de los portales. Para este diseño se examinaron los requerimientos de Transmilenio, se analizó los diferentes estándares WIFI con el fin de escoger el más adecuado para la solución, se indagaron estándares de seguridad con el fin de dar una solución con un buen nivel de seguridad, ya que uno de los requerimientos de esta solución era que el estándar de cifrado a utilizar fuera el WEP y como ya se sabe este estándar no ofrece un nivel de seguridad muy alto, por esto se busco otro nivel de seguridad para asegurar los datos de Transmilenio. En este caso se concluyo que la mejor opción era utilizar el Filtrado de direcciones MAC para ofrecer una buena seguridad a los datos que se produjeran del PAU a la sede Administrativa y viceversa.

Para la selección de los equipos a utilizar el factor que predomino fue el de Costo-Beneficio, en este caso los 3 equipos evaluados tenían muy buenas características y cualquiera de los que se escogiera cumplía con los requerimientos que exigía la solución, pero en la práctica uno de los factores que más predomina es el de costo, y en esto el Acces Point Allied Telesyn tenía el mejor factor de Costo-Beneficio. También se utilizaron antenas QP-COM y PoE de la marca D-Link, ya que estas marcas ofrecen un buen rendimiento y a un excelente precio.

Finalmente se presento una solución que satisfacía todos los requerimientos y en este trabajo se muestra los pasos que se siguieron para diseñar la solución y para su implementación.

Se muestran imágenes de los puntos escogidos para el montaje de las antenas y se ilustra las configuraciones realizadas en los Acces Point de cada uno de los portales.

Referente a la experiencia adquirida en la práctica puedo decir que gracias a esta logré afianzar muchos conocimientos adquiridos en mis estudios y además aprendí aspectos importantes.

En la relación real con la ingeniería en el campo laboral es muy importante tener en cuenta el hecho de poder solventar de forma rápida los problemas que el cliente necesita solucionar cumpliendo con todos sus requerimientos.
En esta práctica también pude aprender que no siempre la solución más cara es la mejor, y ahí es donde entra el papel del ingeniero, en el hecho de dar soluciones eficientes independientemente de lo que se tenga, en muchas ocasiones los problemas se presentan en redes que ya están completamente montadas y el papel del ingeniero esta en poder dar solución a cualquier problema sin importar que equipos o dispositivos se posea el cliente.

8.0 RECOMENDACIONES

Para realizar un diseño que cumpla con las necesidades exigidas se debe realizar una reunión previa con el personal encargado de la red para conocer de forma detallada los requerimientos y así ofrecer la solución que el cliente espera.

Cuando por causas de fuerza mayor no se pueda implementar el método de seguridad más recomendado, se aconseja darle otro nivel de seguridad a la red Wireless, esto con el fin de evitar problemas futuros en la red por causa de espías o intrusos en esta.

Se recomienda al usuario final asegurar los puntos eléctricos, es decir que estos estén regulados o en su defecto tenga algún estabilizador.

Es importante recordar que en la práctica el factor más importante siempre va a ser el de Costo-Beneficio, y esto es algo que siempre se va a poder ofrecer de acuerdo a la capacidad y el conocimiento de la persona o empresa que ofrezca la solución.

Cuando el Acces Point soporta PoE se recomienda que al realizar la conexión con el PoE solo se utilice el Terminal modulador ya que si el equipo soporta esta tecnología no es necesario utilizar el demodulador para separar la alimentación de los datos de esta forma la conexión funcionara mucho mejor. Esto se comprobó en la conexión inalámbrica realizada a Transmilenio en la cual se quiso utilizar el demodulador para que el Acces Point recibiera energía y datos por cables separados pero con esto no se obtuvo un buen funcionamiento ya que el Acces Point se Reiniciaba constantemente debido a que el demodulador no entregaba bien la alimentación a el equipo.

9.0 FUENTES DE REFERENCIA

TechLAN Solutions Ltda.

Documentos Internos.

Experiencia Personal Práctica Empresarial.

www.3com.com

www.dlink.com

www.qpcom.com

Ph.D. Barradello, Carlos. Introducción a las Redes Wi-Fi: *Los Estándares Técnicos 802.11 b/g/a*, Volumen 1 Número 2, Noviembre 2003. Disponible en internet: <URL:http://www.icamericas.net/Cases_Reports/Wi-FiBriefs/WiFi2_Spanish.pdf>.

Madrid Molina, Juan Manuel. Seguridad en redes inalámbricas 802.11, Abril 2004. Disponible en internet: <URL:http://www.icesi.edu.co/.../publicaciones/contenidos/sistemas_telematica/3/jamdrid-seguridad_redes_inalambricas.pdf>.

Dr. Meléndez Lagunilla, Juan y Dr. Bistué García, Guillermo. Metodología de Diseño de PLLs Aplicada al Desarrollo de un Sintetizador de Frecuencia Integrado CMOS para el Estándar de WLAN IEEE 802.11ª, Julio 2006. Disponible en internet: <URL: http://www.tecnun.es/Tesis/orden/electronica/electro39.htm>.

Barajas, Saulo. Protocolos de seguridad en redes inalámbricas. Disponible en internet: <URL: http://www.saulo.net/pub/inv/SegWiFi-art.htm>.

www.es.wikipedia.org

http://www.gammainternet.com/tecnologia/wireless/glosario.html#802.11

ANEXOS

ANEXO A. CARACTERÍSTICAS ACCESS POINTS EVALUADOS EN LA SOLUCIÓN

3Com® Wireless LAN Access Point 8750

Código 3CRWE875075A

Soporta funcionamiento de access point cuando se utiliza con los switches o controllers **3Com** wireless LAN.

Permite acceso rentable a la red a los edificios remotos del campus con soporte para Wireless Distribution Systems (WDS).

Permite dar servicio a diferentes grupos de clientes mediante un único access point que puede actuar virtualmente como dos puntos de acceso físicos.

Se distribuye como punto de acceso bi-direccional 802.11a-802.11g para soportar a más clientes inalámbricos dentro de la misma área de cobertura.

Soporta hasta 253 usuarios simultáneos a velocidades de hasta 54 Mbps y distancias de hasta 100 metros (328 pies).

Clear Channel Select escoge el canal menos traficado para brindar conexiones sin problemas.

La conexión automática a la red y los cambios dinámicos de velocidad hacen que las conexiones a la red estén continuamente disponibles modificando las velocidades de conexión automáticamente, a medida que las condiciones cambian y los usuarios móviles se desplazan a través del área de cobertura de la red.

A través de PoE el punto de acceso recibe corriente por medio de cables Ethernet existentes, resultando en instalaciones más simples y flexibles; no se requiere un suministro de potencia adicional.
Una antena de radio diversa provee rendimiento y cobertura excelentes en ambientes de altas trayectorias múltiples tales como oficinas, bodegas y otras instalaciones internas.

Las opciones de antenas externas extienden el alcance de la conexión inalámbrica 802.11g a hasta 305 metros (1,000 pies).
Se distribuye como punto de acceso 802.11g 2.4 GHz de una sola modalidad de 54-Mbps con una ranura abierta de radio intercambiable.
Soporta a usuarios inalámbricos 11g y 11b, preservando sus inversiones inalámbricas existentes.
La encriptación WEP de clave compartida de 40/64 bits y 128/54 bits, y la encriptación avanzada WPA AES de 256 bits asegura la privacidad de todas las transmisiones inalámbricas.

El enlace dinámico de seguridad automáticamente asigna claves de encriptación específicas para cada usuario de 128 bits en las sesiones inalámbricas.
La autentificación 802.11x del servidor RADIUS controla el acceso a la red inalámbrica y centraliza la autorización de los usuarios en toda la red.
La administración dinámica de claves de sesión y la asignación de claves dinámicas TKIP mejora la seguridad y simplifica las implementaciones
Las listas de control de acceso de direcciones MAC controlan el acceso a los recursos de la red.
Las funciones de filtración "cliente a cliente" y filtración de uplinks dirigen las comunicaciones entre otros usuarios inalámbricos asociados a los puntos de acceso.

La asignación dinámica de VLAN, utilizada con autentificación RADIUS, les provee a los usuarios a una VLAN adecuada, protegiendo aún más el acceso a los recursos de la red.

El soporte para SNMP, **3Com** Network Supervisor y otros software de gestión basados en estándares asegura una integración sin fisuras con su red de cable.

Las herramientas Wireless Infrastructure Device Manager (Gerente Inalámbrico de Infraestructura de Dispositivos) y Wireless LAN Device Discovery. (Descubrimiento de Dispositivos en LANs Inalámbricas) permiten configurar parámetros, ejecutar diagnósticos y supervisar el rendimiento desde cualquier punto en la red, usando un navegador Web.

Soporte para SNMP, **3Com** Network Supervisor, HP OpenView y otros software de administración basados en estándares, aseguran una integración ininterrumpida con su red por cables.

El soporte de contabilidad RADIUS permite facturación por uso de hotspot u otro tipo de implementaciones comerciales.

La herramienta de detección de sitios funciona con PC Cards empresariales inalámbricas de **3Com** para ayudarle a optimizar la localización y el número de puntos de acceso de su instalación.

Especificaciones Técnicas.

- **Usuarios Soportados:** Hasta 253 usuarios simultáneos
- **Cumplimiento con estándares:** Certificación Wi-Fi, IEEE 802.11a, IEEE 802.11g
- **Velocidades de datos:** 802.11a: 54, 48, 36, 24, 18, 12, 9, 6Mbps (hasta 108 Mbps en modalidad turbo) 802.11g: 54, 48, 36, 24, 18, 11, 9, 5.5, 2, 1 Mbps
- **Banda de frecuencia:** 802.11a: 5 GHz 802.11g: 2.4 GHz

- **Medio inalámbrico:** 802.11a: OFDM, 802.11g: OFDM y DSSS (con codificación Barker y CCK para compatibilidad con el estándar anterior 802.11b)
- **Protocol de Acceso de Medios:** CSMA/CA
- **Canales operativos:** 802.11a: 36 - 64 (total de 8) 802.11g: 1 - 11 (EUA y Canadá), 1 - 13 (en todo el mundo; la disponibilidad del canal depende de regulaciones locales)
- **Alcance operativo:** 802.11a: hasta 50 metros (164 pies) de transmisión y recepción 802.11g: hasta 100 metros (328 pies) de transmisión y recepción
- **Configuraciones de potencia de transmisión:** 802.11a: 17 dBm en banda baja dependiendo de la velocidad en bits; 20dBm en banda media dependiendo de la velocidad en bits; 802.11g: 17 dBm dependiendo de la velocidad en bits
- **Consumo:** 2W de media, 11,2W máximo
- **Sensibilidad de recepción:** 802.11a: 6 Mbps: -84 dBm, +/- 2 dBm (dependiendo de la banda) 12 Mbps: -82 dBm 36 Mbps: -73 dBm 54 Mbps: -66 dBm 802.11g: 1 Mbps: -96 dBm 2 Mbps: -94 dBm 5.5 Mbps: -92 dBm 11 Mbps: -88 dBm 12 Mbps: -86 dBm 24 Mbps: -85 dBm 36 Mbps: -80 dBm 54 Mbps: -73 dBm
- **Seguridad:** Encriptación WEP de 40/64 y 128/154 bits; encriptación WPA AES de 256 bits, encriptación Dynamic Security Link de 128 bits; 802.11x con autentificación de servidor RADIUS; autentificación EAP-MD5, EAP-TLS, EAP-TTLS y PEAP; ESSID broadcast control, autentificación MAC local; listas de control de acceso a servidores, administración de Sesiones Dinámicas de Claves y TKIP, asignación dinámica VLAN, filtración cliente a cliente y uplink
- **Rendimiento:** Clear Channel Select, conexión automática a la red, cambios dinámicos de velocidad

- **Gestión de red:** Herramienta para "Site survey", Wireless Infrastructure Device Manager, Wireless LAN Discovery Tool, 3NS, SNMP
- **Seguridad:** IEC & EN 60950, UL / CSA 60950, NOM 019
- **RF:** FCC Parte 15.247, Parte 15.205, Parte15.209, y Parte 15.407, RSS-210, EN 300 328-2, EN 301 893, TELEC RCR STD 33 & T66
- **EMC :** EN 301 489-17, EN 301 489-3
- **Alcance de operación ambiental:** Temperatura de operación: 0°C a 40°C (32°F a 105°F); Humedad: 5-95% no-condensación
- **Antena:** 802.11a: Antena integrada solamente; 802.11g: Opciones de antena externa disponibles, ver Lista de Opciones para mayores detalles
- **Dimensiones:** Alto: 32 cm (12.5 pulgadas) Ancho: 20 cm (8.1 pulgadas) Profundidad: 7 cm (2.8 pulgadas)

Cisco Aironet 1300 Series Outdoor Access Point or Bridge

FEATURES

The Cisco Aironet 1300 Series access point or bridge provides the following features.

Antenna Alignment Assistance

The autonomous Cisco Aironet 1300 Series provides an autoconfiguration and installation mode for quick deployment of point-to-point links without the need for configuration through Telnet, FTP, or Simple Network Management Protocol (SNMP). This mode provides LEDs with signal-strength information used in the installation and alignment process. As a result, installers are free to perform their installation process and verify the link quality without knowledge of Cisco IOS Software or data networking.

Automatic RF Configuration

Under the Cisco Unified Wireless Network, radio resource management provides automatic configuration of RF parameters for access points such as the Cisco Aironet 1300 Series Access Points. The result is a coordinated RF plan for access points under the span of the Cisco wireless LAN controller, which also recognizes the presence of other RF emitting devices. This minimizes interference to and from neighboring access points, ensuring optimal network capacity.

Seamless Layer 2 and Layer 3 Roaming

The Cisco Aironet 1300 Series provides fast secure roaming of wireless clients and autonomous non-root bridges and workgroup bridges. In both the unified access point and the autonomous access point, the encryption keys for mobile devices are cached locally, allowing the mobile device to roam between access points while remaining authenticated to the network. This significantly reduces roaming time by

eliminating the need to conduct the four-way handshake with each roam. Autonomous non-root bridges and workgroup bridges also scan in the background to search for alternative Cisco Aironet access points and bridges that mobile device may be roaming to, which also reduces roaming time.

Support for Port Aggregation Protocol and Cisco Fast EtherChannel Technology

Bandwidth can be increased between bridged networks through the aggregation of multiple autonomous bridges at each site via Cisco Fast EtherChannel® technology, Port Aggregation Protocol (PAgP), or routing protocols.

Wireless Link-Distance Adjustment

For an autonomous Cisco Aironet 1300 Series device, the link-distance parameter allows the user to tune the Carrier-Sense Multiple Access/Collision Avoidance (CSMA/CA) parameters for the particular range in use to maximize performance.

Wireless Packet Concatenation

The concatenation of smaller packets into larger ones allows autonomous Cisco Aironet 1300 Series access point or bridge to more efficiently use the wireless medium and provide higher overall data throughputs.

Wireless Programmable Clear-Channel Assessment

With a programmable clear-channel assessment, an autonomous Cisco Aironet 1300 Series access point or bridge can be configured to the particular background-interference level found in your environment. This provides reduced contention overhead with other wireless systems.

Protocols.

Air Interface Standard: IEEE 802.11b or IEEE 802.11g

Note: Autonomous bridge mode has enhancements to the standard to allow longer-range bridging communications.

Frequency Band: 2.412 to 2.462 GHz (FCC)

· 2.412 to 2.472 GHz (ETSI)

· 2.412 to 2.472 GHz (TELEC)

Wireless Modulation:

802.11b

· Direct Sequence Spread Spectrum (DSSS):

· Differential Binary Phase Shift Keying (DBPSK) at 1 Mbps

· Differential Quadrature Phase Shift Keying (DQPSK) at 2 Mbps

· Complementary Code Keying (CCK) at 5.5 and 11 Mbps

802.11g

· Orthogonal Frequency Divisional Multiplexing (OFDM):

· BPSK at 6 and 9 Mbps

· QPSK at 12 and 18 Mbps

· 16-quadrature amplitude modulation (QAM) at 24 and 36 Mbps

· 64-QAM at 48 and 54 Mbps

Media Access Protocol:

Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA)

Lightweight Access Point Protocol:

A network protocol for lightweight access points that also provides for centralized management.

Operating Channels 802.11b/g:

· ETSI: 13

· Americas: 11

· TELEC (Japan): 13

Nonoverlapping: Channels 3

Security-Bridge Role*:

Cisco Wireless Security Suite, including:

Authentication

· 802.1X support including LEAP to yield mutual authentication and dynamic per-user, per-session encryption keys

Encryption

· Cisco TKIP or WPA TKIP; key hashing (per-packet keying), Message Integrity Check (MIC) and broadcast key rotation

· AES (802.11i)

Security-Access Point Role:

Cisco Wireless Security Suite supporting WPA and WPA2, including:

Authentication

· Management frame protection provides for the authentication of 802.11 management frames by the wireless network infrastructure. This allows the network to detect spoofed frames from access points or malicious users impersonating infrastructure access points. If an access point detects a malicious attack, an incident will be generated by the access points and reports will be gathered on the Cisco wireless LAN controller, Cisco WCS, or CiscoWorks WLSE.

· 802.1X support including Cisco LEAP, Protected EAP-Generic Token Card (PEAP-GTC), PEAP-Microsoft Challenge Authentication Protocol Version 2 (MSCHAPv2), EAP Message Digest 5 (EAP MD5), EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled TLS (EAP-TTLS), EAP-Subscriber Identity Module (EAP-SIM), and EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) to yield mutual authentication and dynamic per-user, per-session encryption keys

Encryption

· WPA: Cisco TKIP or WPA TKIP; key hashing (per-packet keying), MIC and broadcast key rotation

· WPA2: AES (802.11i)

Security-Workgroup Bridge Role*:

Cisco Wireless Security Suite, including:

Authentication

· 802.1X support including Cisco LEAP to yield mutual authentication and dynamic per-user, per-session encryption keys

Encryption

· Cisco TKIP or WPA TKIP; key hashing (per-packet keying), MIC and broadcast key rotation

· AES (802.11i)

SNMP Compliance Versions 1 and 2

* The Cisco Aironet 1300 Series can operate as a workgroup bridge or wireless bridge when it is an autonomous device. When the Cisco Aironet 1300 Series is operating under the Cisco Unified Wireless Network architecture, it only operates as an access point.

Dual-radio Enterprise-class Wireless LAN Access Point

AT-WA7400

Key Features

• High-performance 54Mbps (802.11a/g) data rate

• Security support via 802.11i (WPA2), WPA-PSK,TKIP,AES, IEEE 802.1x, and EAP/802.1

• Multiple BSSID and Virtual LAN (VLANs)

• Inhibit SSID broadcast and Ignore SSID scan

• Media Access Control (MAC) for wireless Interface

• Load Balancing

• 802.11e (WMM only)

• Wireless Distribution System (WDS) for Wireless Bridge and repeater modes support

• AP Clustering

• Rogue AP detection

• Transmit Power Control/limiting

• Secured AP management

• Power-over-Ethernet capable

• Wi-Fi and WPA certified

Wireless Radio Characteristics

IEEE 802.11g Wireless Radio

Frequency Band: 2.4GHz, actual frequencies vary by

country

Radio Type: IEEE 802.11b (11Mbps) and IEEE 802.11g: (54Mbps)

Modulation: 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)

• PSK @ 6 and 9 Mbps

• QPSK @ 12 and 18 Mbps

• 16-QAM @ 24 and 36 Mbps

• 64-QAM @ 48 and 54 Mbps

• 802.11b and 802.11g: Direct sequence spread spectrum (DSSS)

• DBPSK @ 1 Mbps

• DQPSK @ 2 Mbps

• CCK @ 5.5 and 11 Mbps

Radio Power Output: 12.5~18 dBm depending on frequencies

Radio Data Rate: 54, 48, 36, 24, 18, 12, 9, and 6Mbps OFDM, 11 and 5.5Mbps CCK and legacy 2 and 1Mbps data rates.

Channels: United States (FCC) 11 Channels, Europe (ETSI) 13 Channels, Other countries per local regulations

Wireless Features

Dynamic channel planning

Auto channel selection

Transmit Power Control/Limiting

Wireless Distribution System

Load Balancing

Virtual wireless network via multiple BSSIDs

Management

Management Interfaces: Telnet and Web

SNMP Agent:

SNMPv1 v2c supported

Web-based Management Tool

Single-View of clustered APs

Single-click firmware upgrade

Upload and download text-based configuration file via HTTP browser

Firmware upgrade via HTTP browser

Physical Characteristics

Dimensions: 176 x 101 x 30 mm (W x D x H)

Weight: 250g (.55 lbs)

Security

64, 128, 152 bits WEP, Static and Dynamic Mode

Weak IV Avoidance

MAC Access Control for Wireless interface

EAP and 802.1x support

Open/Shared Authentication

WPA, WPA-PSK Compliant

WPA with TKIP/AES support

Supports IEEE 802.11i (WPA2)

Per-VLAN-based Authentication policy

Inhibit SSID broadcast and Ignore SSID scan

Network Protocol And Standards Compatibility

IEEE802.3 CSMA/CD

IEEE802.3u 100BaseTX

IEEE802.11g

IEEE 802.11i

IEEE802.1x

Draft IEEE 802.11f

Draft IEEE 802.11e

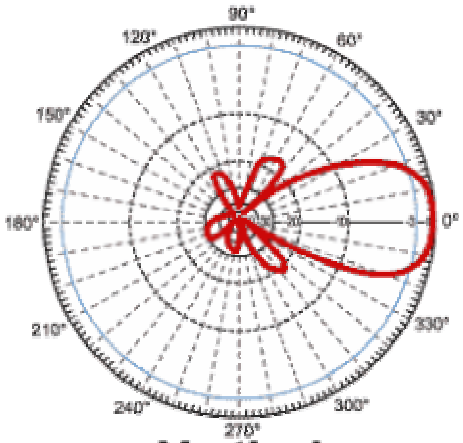
ANEXO B. CARACTERÍSTICAS ANTENAS UTILIZADAS EN LA SOLUCIÓN

ANTENA 14 DBI PANEL 2.4 GHZ

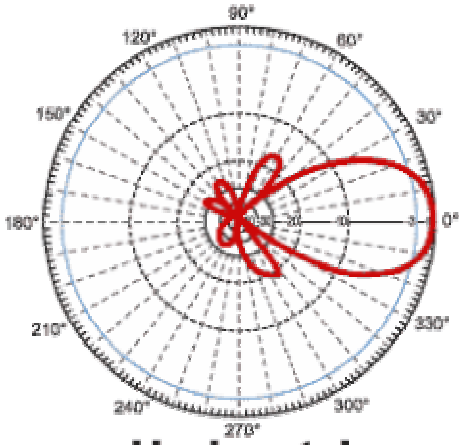
QP-AO14P

Características

The QP-AO14P is a high performance directional flat pacth WiFi antenna suitable for indoor and outdoor applications in the 2.4 GHz ISM band, including IEEE 802.11b and 802.11g wireless LANs, Bluetooth, and public wireless hotspots. This WiFi antenna is light weight and features an aesthetic UV-stable, UL flame rated white plastic radome which can also be painted to match the room or building structure. The QP-AO14P can be installed for horizontal or vertical polarization. It can be wall or ceiling mounted, as well as mast-mounted using U-bolst.



Vertical



Horizontal

Ventajas

- Superior Performance.
- Durable UV- stable, UL flame rated radome.
- 12 inch coax lead.
- Can be installed for either vertical or horizontal polarization.
- Optional mounting brackets available.
- Frequency: 2400-2500 MHz.
- Gain 14 dBi.
- Lightning Protection DC Short.
- Light weight

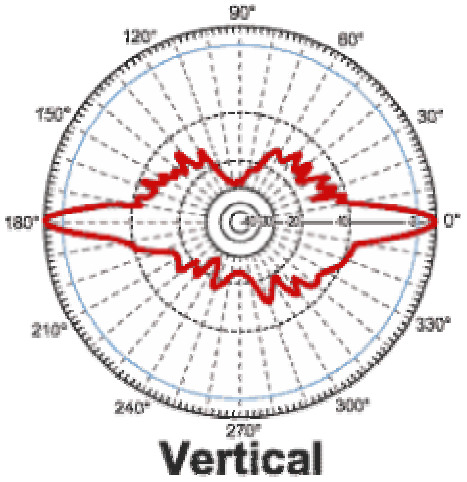
ANTENA 12 DBI OMNI 2.4 GHZ

QP-AO12O

Características

The QP-AO12O is a high gain omnidirectional base station WiFi antenna designed and optimized for the 2.4 GHz ISM ban. This lightweight antenna is ideally suited for IEEE 802.11b and 802.11g wireless LANs, Bluetooth and other multipoint applications where long range and wide coverage is desired.

This WiFi antenna features a 12 inch coax lead terminated with N-female connector. The mounting system consists of a steel bracket and pair of 2.5 inch U-bolts, allowing installation on masts up to 2.0 inches in diameter.



Ventajas

- Frequency: 2400-2500 MHz.
- Gain: 12 d Bi.
- Polarization: Vertical.
- Vertical Beam Width: 8º.
- Horizontal Beam Width:360º.
- Max. Input Power: 50 Watts.

ANEXO C. CARACTERÍSTICAS POWER OVER ETHERNET D-LINK

POWER OVER ETHERNET

DWL-P100

Funcionalidad

- Suministra alimentación (CC) a otros periféricos a través del puerto Ethernet utilizando cableado de categoría 5
- Transforma la corriente CA de entrada en corriente continua CC de bajo voltaje en salida - La unidad Base y la unidad Terminal están conectadas entre sí a una distancia máxima de hasta 100 metros
- Protege a los periféricos, como por ejemplo los puntos de acceso, de posibles daños producidos por la fuente de alimentación.

Especificaciones técnicas

- Pins del cable (Cat. 5) utilizados para la alimentación: 4/5, 7/8
- Voltaje en salida : 5VCC/1A (parte terminal)
- Conector Ethernet : RJ45
- Cable Ethernet : Categoría 5, TIA/EIA-568
- Transmisión de datos Ethernet : 10/100Mbps
- Número de aparatos Ethernet alimentados por el DWL-P100 : 1
- Peso aparatos (par) : 122 g
- Dimensiones : 8 x 4.4 mm

ANEXO D. PLANO PORTAL DE LA 80